International University of Africa
Deanship of Graduate Studies, Scientific Research and Publishing.
Iqra Faculty for Computer Studies.
Department of Information Technology.

Preventing Man in the Middle Attacks in Cloud Environment by Using Cryptography and Video Steganography techniques.

Thesis Submitted in partial fulfillment of the requirements for the degree of Master of Science in Information Technology

BELLO ABDUL-SHAKUR ADEBAYO

Supervised by:
Dr Murtada Malik Adam Elhaj
Assistant Professor – Information Technology.

AH 1440 – 2020


بسم الله الرحمن الرحيم

Dedicated to all Researchers, Students and anyone in need of knowledge.

Acknowledgement

All thanks and praises to Allah who granted me the strength, support and guidance and eased the difficulties, which I faced while preparing this thesis.

I would like to express my deepest gratitude to my great supervisor, **Dr. Murtada Malik Adam Elhaj,** Assistant professor of information technology at the **international university of Africa** who guided, corrected, and gave me a lot of recommendation tirelessly until I was able to accomplish the goals of this research.

I also like to thank **Dr. Ashraf Zubeir,** the dean of **Iqra faculty of computer studies** at the international university of Africa for his continuous words of encouragement and assistance. I also would like to thank all the academic staff at the faculty for supporting me directly and indirectly.

I am greatly indebted to my parents **Mr Muslihudeen Bello** and **Mrs Rahmatallah Bello**, who are always understanding and supportive. They sacrificed all they have to see that I do not suffer academically I express my eternal gratitude to them. Special thanks to my family entirely and others for their supports and advices.

Special thanks to my colleague brother Raji Atoyebi Abdulmajeed who also assisted me largely in the completion of this research.

I cannot forget to thank my colleagues at the Iqra Faculty of computer studies who supported me until the completion of this study.

Bello Abdul-Shakur Adebayo

Abstract

Cloud Computing is currently one of the hottest topics in computing and information technology (IT), it's a technology paradigm that is offering useful services to consumers. Cloud computing is facing a lot of security problem, in order to go against all this problem, the researcher securing cloud environments against unauthorized use/access, distributed denial of service (DDOS) attacks, MITC attacks, hackers, malware, and other risks.

In this study, the main objective is to develop a model for preventing man in the middle attacks while sending the secret messages to the cloud storage, by studying the state of art of security models in public cloud computing and analyzing them, in particular the models for confidentiality of data.

This study used the descriptive, deductive, applied and prototype methodology. We developed a model, where we need to embed secret message before sending to the cloud storage without involvement of third party (Attackers), and extract the secret message after it reached the cloud storage. While embedding the secret message, we used Video steganography and Cryptography techniques; which is LSB and AES encryption, AES is for encrypting secret message and LSB is for hiding encrypted message inside the video frames, after this, stego-video will send to cloud storage. While extracting the secret message, we used both LSB and AES to extract the secret message too. We used several tools and programming languages to implement the model and experiments. Our experiments proved that the model is effective and acceptable.

Among the most important results is that the model provides strong user authentication and it provides confidentiality, it also increases user confidence in cloud applications as we ensured secure connection between cloud users and cloud service providers, and our message is well prevented from man in the middle attacks. Future studies should be conducted to solve the problem of phishing attacks for web pages, and the model can be improved to verify the integrity of files sending to the cloud storage.

مستخلص

تعد الحوسبة السحابية حاليا واحدة من أهم الموضوعات في مجال الحوسبة وتكنولوجيا المعلومات (IT)، وهي نموذج تقني يقدم خدمات مفيدة للمستهلكين. تواجه الحوسبة السحابية الكثير من المشاكل الأمنية، من أجل مواجهة كل هذه المشكلة، نحتاج إلى تأمين البيئات السحابية ضد الاستخدام / الوصول غير المصرح به، وهجمات رفض الخدمة الموزعة (DDOS)، وهجمات MITC، والمتسللين، والبرامج الضارة، وغيرها من المخاطر.

هدفت هذه الدراسة إلى تطوير نموذج لمنع الإنسان في الوسط من الهجمات السحابية (MITC) أثناء إرسال الرسائل السرية إلى التخزين السحابي، وذلك خلال دراسة أحدث نماذج الأمان في الحوسبة السحابية العامة وتحليلها، وخاصة نماذج سرية البيانات.

استخدمت هذه الدراسة المنهج الوصفي والاستنباطي والتطبيقي والنموذج الأولي. قد قام الباحث بناء التطوير نحوه، حيث نحتاج إلى تضمين رسالة سرية قبل إرسالها إلى التخزين السحابي دون أن تكتشفها طرف ثالث (المهاجمين)، واستخراج الرسالة السرية بعد وصولها إلى التخزين السحابي. أثناء تضمين الرسالة السرية، استخدمنا تقنيات تشفير المعلومات وإخفاءها بالفيديو؛ وهو تقنية LSB وAES، وAES مخصص لتشفير الرسائل السرية وLSB لإخفاء الرسائل المشفرة داخل إطارات الفيديو، بعد ذلك، سيتم إرسال stego-video إلى التخزين السحابي. أثناء استخراج الرسالة السرية، استخدمنا كلاً من LSB وAES لاستخراج الرسالة السرية أيضا. استخدمنا عدة أدوات ولغات برمجة لتنفيذ النموذج والتجارب. أثبتت تجاربنا أن النموذج فعال ومقبول.

من أهم النتائج أن النموذج وفر مصادقة قوية للمستخدم ووفر كذلك السرية، كما أنه يزيد من ثقة المستخدم في التطبيقات السحابية حيث عملنا على ضمان الاتصال الآمن بين مستخدمي السحابة ومقدمي الخدمات السحابية، وتم منع رسالتنا جيدا من الرجل في الوسط الهجمات. يجب إجراء دراسات مستقبلية لحل مشكلة هجمات التصيد لصفحات الويب، ويمكن تحسين النموذج للتحقق من سلامة الملفات المرسلة إلى التخزين السحابي.

Table of content

Contents

List of figures

List of tables

List of Abbreviations

LSB – Least Significant bit.

AES- Advanced Encryption system.

s-key – secret key

MICT- Man-in-the cloud attacks.

IP – internet protocol.

HTTP - hypertext transfer protocol.

CIA- Confidentiality, Integrity, Availability.

AWS – Amazon Web Services.

Chapter (1):

Introduction

,

Chapter 1

1.1 Introduction

Internet is driving force towards the different technologies that have been developed. One of the most discussed among all of these is cloud computing. Over the last few years, cloud computing paradigm has a drastic and enormous shift towards its adoption and it has become a trend in Information Technology as it promises significance cost reduction and new business potential to its users and providers. The concept of Cloud Computing was introduced back in 1960s by John McCarthy. According to him "computation may someday be organized as a public utility" [2].

Cloud computing is a kind of computing technique where IT services are provided by massive low-cost computing units connected by IP networks [1]. The cloud services can be accessed with different kinds of devices e.g., Network, Notebook, tablets, Pc, Server, etc. as shown in fig 1.1.

Fig 1.1- Cloud computing overview

Fig 1.2- Cloud's service and deployment model.

As shown in fig 1.2 at the topmost layer of the figure, they go on to then list three service models which should be already familiar to most observers: Software as a service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Finally, they list four possible deployment models for cloud computing: **private cloud, community cloud, public cloud and hybrid cloud,** while shown in fig. 3 the five essential characteristics are: on demand service, brand network access, resource pooling, rapid elasticity and measured service [3].

Fig. 1.3 Five essential characteristics of cloud computing

Virtualization is the backbone of Cloud Computing; Cloud computing brings efficient benefits as well as makes it more convenient with the help of Virtualization, not only this, it also provides solutions for great challenges in the field of data security and privacy protection. Virtualization is the imitation of hardware within in a software program. A Single computer is allowed to perform the role of multiple computers. It uses in cloud computing: for Combining local and network resources data storage virtualization. For grouping physical storage devices into single unit, Capacity improvement [4].

1.2 Problem Statement

With the present wide furtherance of cloud computing services, processing and storing of large amount of data and information in the cloud, this poses challenge to the CIA triad, Attacks like man in the cloud attack is a popular method attackers use to intercept transmission of information between the cloud user and provider, with such attack the attacker can have access to confidential information or make changes without the knowledge of either the cloud user or cloud service provider. Cloud users need to be assured of the trustworthiness of cloud services and that their data/information are transferred safely over the internet.

In short, we need to adopt more reliable techniques for transmission of data/information to the cloud so as to prevent unauthorized access to cloud user data/ information. In this study, we will study the man-in-the cloud attack works and we will propose a more secure model.

1.3 Objectives

1.3.1 General Objectives

The general Objective of this is to build an application that will improve the confidentiality and integrity of user and data in cloud environment in order not to access by middle attacker.

1.3.2 Specific Objectives

1. To study the state of art of man-in-the cloud attacks in cloud environment.
2. To propose Security model for cloud computing and implement it.
3. To implement and evaluate the proposed model to function with a acceptable performance.
4. To accumulate deep-rootedness of confidentiality in cloud computing.

1.4 Research Questions

1. What are the current existing hiding techniques in cloud computing?
2. What is the weakness of the existing hiding techniques?
3. What is the possible solution to existing hiding techniques in cloud computing?
4. Does the cloud computing allow encryption and hiding of information between the parties in cloud environment?
5. How does man in cloud attack operates in the cloud?

1.5 The significance of the research

The study will analyze the existing hiding and encryption techniques for transmission of data in the cloud. Users/customer must be assured that while sending or receiving information from cloud provider they are free from the man in cloud attack. This study will propose a model that will help in preventing access to secret message while sending/receiving in the cloud environment.

1.6 Research Methodology.

Research methodology is a process of managing and solving research problem systematically. To achieve the goals of research we will use different methods and techniques, which includes; we begin by studying state of art of cloud security, existing theories and techniques related to research problem area hence deductive approach is used and we will propose a model hence the applied approach then develop a prototype application, so the prototype methodology will be followed:

Step1: Data Acquisition/ systematic literature review: is an act of reviewing the recent related papers about confidentiality of data/user on cloud and studying the existing models in order to achieve on its disadvantages. More so, we find about appropriate algorithms that can be used for hiding secret messages.

Step (2), Analysis and Design:

Cloud provider will send a secret message on cloud, before getting to the user, we need to embed the secret message in a cover file in order not to attack by the middle man, when the user/customer want to check the secret message he/she need to extract the file by having the password sent to him/her by cloud provider.

Step (3), Implementation:

1. Implementation and coding phase of the proposed model using programming languages suitable for public cloud.
2. Upload the written code to Cloud computing for experiments and evaluation.

Step (4), Experiments and Evaluation:

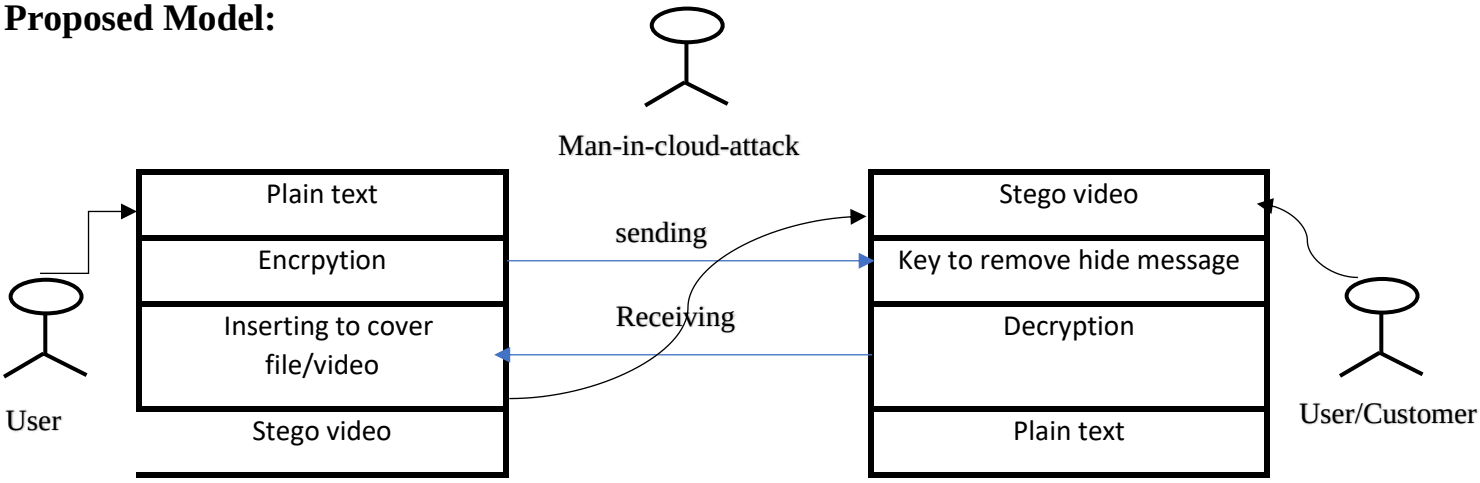
Evaluate the confidentiality of data after sending the files in to the user/customer without attacks by middle-man.

Evaluate the capacity of cover data after hided secret message into it.

1.7 Research tools:

The thesis is written based on scientific papers, online sources, journals etc. To get relevant papers, we searched mostly the following databases: ResearchGate and Google Scholar, IEEE, and from another websites. We looked for the Keywords "cloud computing", "cloud security", "man-in-cloud-attack", "steganography", "CIA cloud computing" in titles, abstracts or keywords of reviews/articles and we also use some analysis application e.g Visual Paradigms, Python language, Microsoft Office word.

Proposed Model:



1.8 Research Scope.

The thesis focuses on analyzing the techniques used for hiding secret messages in the cloud without access by man-in-cloud-attack, we will further establish the current state of art for ensuring the correctness of previous models.

Time scope: This research will hold from March 2021 to June 2021.

1.9 Research Structure

We will divide this research into 5 sections, **Chapter (1), Introduction:** which will contain the research proposal. **Chapter (2), Literature review and Related Works:** In this chapter we will discuss the overview in cloud computing, also we will discuss overview of security in CC cloud security, Man-in-Cloud attack, Cryptography, Steganography, and presents most previous related works and explains points of differences and Similarities. **Chapter (3), Methodology (Analysis, Design and Implementation):** we will present model for preventing man-in-cloud from attack in cloud with its architecture and the main functions and basics of the model. Then Implementation. **Chapter (4), Testing and Evaluation:** Build Sample system based on model, the experimental works, evaluating and analyzing the experimental results. **Chapter (5), Conclusion and Future Work:** we present Discussions, Conclusions, recommendations, future works.

Chapter (2):

Literature review and Related Works

Chapter 2

2.1 Introduction

firstly, we will overview the cloud computing which involves definition, characteristics, delivery models and deployment models, benefits, risks and obstacles preventing Adoption of Cloud computing, factors affecting performance, Cloud computing Reference Architecture. **Secondly,** we will overview the security in CC, Cloud security issues and threats, Security goals and requirements, Confidentiality in cloud, Cloud security existing solution. **Thirdly,** we will discuss briefly about the man- in-cloud Attack. **Fourthly,** we will overview cryptography which include the definition and origin of encryption techniques, how encryption works, popular encryption system. **Fifthly,** we will discuss steganography which involve definition, and techniques **sixthly,** we will list some related works which are more similar to our work.

2.2 Background Information:

Cloud Computing has been capturing the interest of many organizations as well as academic entities due to its cost effectiveness and capabilities, Despite Cloud technology being adopted across the world, there is less literature on its security issues and the increase in Cloud attacks [5]. In this study we will present an analysis of different techniques used to preventing any attacks in cloud, especially middle attacker, and comparing them with previous studies, then suggest our possible model.

The diversity of Cloud computing models possesses a security risks where different types of attacks are now targeting the Cloud infrastructure [7]. The most predominant Cloud attacks are the Distributed Denial of Service (DDoS) or DOS attacks, and Man-in-the-Cloud (MitC) attacks [5]. The Study will focus on Man-in-the-Cloud (MitC) attacks. MitC attacks are similar to MitB (Man-in-the- Brower) attacks. The difference is that tokens are stolen instead of account credentials. Tokens are used heavily in the cloud apps as authentication mechanisms for transmitting data to cloud app application program interfaces (APIs) from authorized resources. Malware residing in the end-user system is capable of hijacking the communication channel. This is done by either hooking the cloud agent functions or using social-engineering attacks to inject attacker-supplied unauthorized synchronization tokens so that valid and unexpired tokens can be extracted to gain access to users' accounts. Primarily,

the MitC malware exploits the file synchronization services for installing additional malware, exfiltrating data and performing command and control (C & C) operations. The attack is different, but the end result is the same: gaining access to user accounts [6].

Security in Cloud computing is major concern, especially in deployment models and cloud service delivery models. The international Standards Organization (ISO), defines Information Security concerns which can also be guided in regard to the cloud computing key security requirements for an effective and secure technology solution. These are defined as follows: **Confidentiality:** means keeping users' data and allowing privileged entities only to have access to data. **Integrity:** means to assure that there is no alteration or modification in data while it is stored or being transported and only authorized user have access to change, modify, copy or delete data. **Authentication:** means to assure the identity of the user before giving access to data and this can be done by employing certain protections to their profiles. **Availability:** Means Data should be available for authorized users at all times. The user must also have control over their data [8]. **Authorization:** means to assure that the users who have requested the particular information have the right to access it [10].

Fig 2.1 illustrates cloud computing key security requirement coupled with cloud computing deployment models and cloud computing service delivery models and can be seen in context as a guideline to assess the security level. Compulsory requirements are represented by the "✓" symbol and optional requirements are represented by the "×" symbol.

Cloud Computing Key Security Requirements	Cloud Deployment Models	Private/Community Cloud			Public Cloud			Hybrid Cloud		
	Confidentiality	✓	✓	×	×	✓	×	✓	×	×
	Integrity	✓	✓	×	✓	×	✓	✓	✓	✓
	Authentication	✓	×	✓	✓	×	✓	✓	×	×
	Availability	✓	✓	✓	×	✓	✓	×	×	×
	Accountability	✓	×	×	✓	✓	✓	✓	×	×
	Cloud Service Delivery Models	SaaS	PaaS	IaaS	SaaS	PaaS	IaaS	SaaS	PaaS	IaaS

Fig 2.1. Key security requirements coupled with cloud computing deployment models and cloud computing service delivery models. [9]

As shown in Fig4, if a cloud service provider can maintain all the key security requirement in cloud, all data and secret messages in cloud are considered secured.

Security threats in Cloud computing: Apart from the advantages that cloud computing offers, there exist numerous security threats that preclude consumers from enchanting these advantages, among them are: Data Loss, Data Breaches, Account or Service Hijacking, Insecure Interface and APIs, Malicious Insiders, Shared Technology Issues, etc.

Cryptography and Steganography: Cryptography is the art and science of hiding information or data from unintended users [11], some examples of symmetric and asymmetric cryptographic algorithms are: Data Encryption Standard (DES), Rivest Shamir Adleman (RSA) etc... While Steganography**:** comes from the Greek words Steganos (Covered) and Graptos (Writing). The term Steganography came into use in 1500‘s after the appearance of Trithemius book on the subject Steganographia the word Steganography technically means covered or hidden writing. Its ancient origins can be traced back to 440 BC. In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves. Invisible ink has been in use for centuries for fun by children and students and for serious espio-nage by spies and terrorists The majority of today‘s steganograph-ic systems uses multimedia objects like image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication In modern approach, depending on the nature of cover object, steganography can be divided into five types: Text Steganography, Image Steganogra-phy, Audio Steganography, Video Steganography and Protocol Steganography. So, in the modern age so many steganographic techniques have been designed which works with the above con-cerned objects. With respect to Steganography there is a problem of unauthorized data access [12].

In this research we will study the art of hiding data or information from man attacks in cloud computing, available models maintaining man attacks in cloud computing and propose more efficient model.

2.3 Cloud computing Overview

2.3.1 Cloud computing.

The Cloud computing has been defined from different perspectives since it is still at an exploring stage [17]. The National Institute of Standards and Technology (NIST) have proposed a basic concept of cloud computing that is commonly accepted by public [18]. They define cloud computing as a model that allows the sharing of many computing resources as a

service to various clients. In this model, clients can easily change or adjust their service requirements at a low cost. Armbrust and his colleagues' [19] definition of cloud computing is that services are provided by delivering both applications and system's software's in the datacenter, which particularly emphasizes the significance of services in cloud computing. The Clouds in cloud computing includes both software and hardware in datacenter that are usable and accessible virtualized resources [19][20]. Buyya [21] clarifies the difference between cloud computing and two other computer paradigms, cluster computing and grid computing. Cloud computing is not a simple consolidation of cluster computing and grid computing; it is a new-generation of data center that emphasizes virtualized nodes in the systems. Vouk [23] presents that cloud computing will be the next evolution of on-demand IT services and products, which can be engaging through service-oriented architectures (SOA). Linthicum [22] further describes the complementary relationship between cloud computing and SOA. In principle, SOA, a strategic framework of technology, utilizes cloud computing that provides IT resources. Due to former research on Cloud computing, a clear definition of cloud computing has been given by researchers. **Cloud computing is an approach of information sharing or services on both Internet and Intranet; Clients can decide which information or services they are going to use, depending on the clients' demands.**

2.3.2 Characteristics of Cloud Computing:

To help highlight this portion of cloud computing, consider the characteristics identified by NIST in their definition paper for better understanding of its characteristics:

1. On-demand self-service
2. Broad network access
3. Resource pooling
4. Rapid elasticity
5. Metered service metrics

You can get more explanation from the paper written by Christopher Olive [24] as stated below:

A. On-demand self-service

The first characteristic is one of the easiest to define. It simply requires these two things to be true:

1. The service must be always available (or some reasonable approximation of always).
2. The service received must be modifiable by the client organization without contacting the hosting provider.

It is the second that is typically the most difficult to meet. While the public providers like Amazon, Google, and Microsoft have this facet, smaller niche providers typically do not. This is more likely when the provider is also supplying services or managed hosting for the application itself, especially during an Infrastructure as a Service (IaaS)- type scenario. In enterprise application hosting scenarios, there are also potential contractual issues to consider when decreasing (or even possibly increasing) capacity without interacting with the vendor. It is important to determine these issues before making changes to your own environment. If your service/uptime SLAs require a certain level of hardware to support, remember to ensure that you do not compromise them by unduly changing the capacity available to your applications.

B. Broad network access

In this context, broad network access means that the hosted application should be reachable via nearly any network-based appliance. These can include, but are not limited to, the following:

1. Laptop
2. Desktop
3. Smartphone
4. Tablet device

Broad network access is typically accomplished by using the built-in web browser for the device, as it is one of the most ubiquitous clients available. It is not the only client, as the virtual desktop (beyond the scope of this document) requires more specialized software, but it is one of the most commonly selected clients. The advantage of this setup is that client devices can be much less powerful as "thin-clients" rather than "fat-clients" (read this as needing to install software on the client to make it work).

In the early '90s, companies were migrating away from "dumb terminals" that were directly connected to the heavy iron of a mainframe or minicomputer, and going with desktop-based, PC-type machines. This is exactly the opposite of what we see here, as the pendulum swings back in favor of lighter clients, with the cloud replacing the big iron.

C. Resource pooling

Resource pooling is the concept that multiple organizations can share the underlying physical cloud infrastructure. This allows significantly greater purchasing power for these companies because they can typically obtain access to a larger pool of resources rather than procuring the physical or virtual infrastructure themselves.

Typically, user organizations of similar security levels or needs are grouped together on a particular community cloud offering (all federal organizations, all pharmaceutical organizations, all general availability organizations, as examples, live on separate physical cloud infrastructures).

This is typically one of the more difficult paradigms shifts for security professionals. The concept of shared infrastructure (at any level) is not considered as being secure. Since the underlying infrastructure is shared in this scenario, alarm bells usually go off in the heads of the assigned security personnel. However, the hypervisor takes steps to isolate the virtual machines running on it, and there are several layered approaches that can added. This approach combines both new and traditional security measures, some of which are highlighted as follows:

1. Hypervisor products can usually include other plug-in objects to assist in security. VMWare and Microsoft make these for their own products, usually folded into the core offering, and other third-party tools can be used as well.
2. Adding in Network Intrusion Detection software (like SNORT) to listen on the traffic between virtual machines (VMs) is critical, as they do not usually communicate on the external network topology like traditional servers.

3. Adding in VM-based virus scanning to look at the underlying physical files allows more cost-effective anti-virus protection.

4. Updating policies and procedures to address the additional steps necessary for employees to deploy cloud and virtualization is a key component to successful resource pooling.

With proper protocols and procedures, security risks can be mitigated and allow even higher-level security operations in the cloud.

The full range of security steps necessary is outside the scope of this document, but adoption of virtualization by security personnel in the federal space is increasing with

such research as the CDW Server Virtualization Life Cycle Report showing that, while adoption is slower than commercial progress, federal IT personnel are embracing virtualization and the cloud.

D. Rapid elasticity

Rapid elasticity is (nearly) exactly what it says on the tin.

This is the ability to handle spikes in usage at least semiautomatically. While this is something you could technically obtain with physical hardware, the turnaround time

necessary for implementation typically pushes that solution outside the bounds of the definition of the word “rapid.” For example, if the application typically sees between 1,000 and 2,000 users a day, but at certain times of the week/month/year there are more users, you usually have to provision the application to handle the spikes in usage.

This allows you to handle these sudden (or perhaps not so sudden) upticks in usage.

With a cloud-based application, you do not need to account for these spikes as widely. Typically, you would provision your application service for the usual level of concurrence.

Then, one of two things might happen:

1. There is an anticipated spike in usage. For example, you have an application that has to be used by everyone in your organization to handle training during a three-month window.
2. A sudden, unanticipated surge in usage within a small time period occurs. Perhaps you are delivering information that happens to go viral across the larger Internet.

Prior to the option of a cloud-based application, meeting unanticipated demand (and even anticipated demand) required far more planning and cost. You either had to have servers sitting fallow, waiting to be swapped into the pool, or pay for overcapacity to handle the surges.

With cloud services, you can simply plan with your hosting provider to increase capacity during anticipated peaks, with the new (likely virtual) servers provisioned and deprovisioned for you and not remaining inactive during the rest of the year. Alternately, during a period of unanticipated load, your provider may have configured your system to automatically grow when usage reaches a certain threshold, creating and adding virtual servers to your service with a set of scripts, and then removing them in the same way when the demand hits a certain floor.

The second is a more advanced cloud offering and is not available with very many providers; however, it is becoming more of an option.

E. Metered usage

Metered usage is also a straightforward idea: you only pay the hosting provider for the resources you consume. This makes IT more of a utility service you pay for as opposed to the traditional cost models, where you might pay some dollar figure a month to host X number of servers. However, when metered usage is applied to more complex deployments of applications, it can become muddled.

The sticking point comes when one tries to define use. Simply put, metered usage may be the concept of "$X per minute or hour your server is powered on," and this is how most public cloud providers operate. This is an issue when one is looking to host an application that is needed 24x7, when there is no significant cost advantage to having a cloud-hosted solution (there are technical and service advantages, but we are isolating cost for this example).

From here, one may consider moving to a more granular charging fee from the hosting provider. But then we have to consider what use is. Is it sending or receiving an email in a cloud-hosted Exchange service? Is it per report run for an analytical business intelligence application? Or perhaps it's per learning completion in a Learning Management System (LMS). We then have to consider the different weights; should an email with a 2MB attachment "cost" the same as a simple text one? Should a simple report be equal to a financial end-of-year statement report? How would we accommodate other types of users and charge appropriately for an LMS? These situations can complicate the overall seeming ease of this characteristic [24].

2.3.3 Cloud delivery model.

Cloud supports XaaS (Everything as a Service), but offers its services as three majors service models recognized as IaaS, PaaS and SaaS [25]. To deliver cloud services to consumers we need to make use one at of these models available in cloud environment, in other to make interaction easier with consumer. We need to discuss three common models in details which are as follow:

1. **Infrastructure as a Service (IaaS)**

This service model delivers computer infrastructure as a service. This service is made available

as a platform for virtualized machines. Unlike, traditional hardware machines which require special maintenance and limited flexibility, cloud makes these machines easily available virtually on the internet with flexible specifications and improved performance, optimized according to the requirements of the customer.

Developers can run the platforms necessary for their software development and run them. This service also makes it easy for the customer to create instance for his required virtual machine simple and easy. In most of the cloud services provided by various service providers, setting up of virtual machines can be done with no or less cost. Cloud provides this virtualization feature in the form of containers. A direct virtual machine needs a hypervisor on its hardware above the kernel for efficient virtualization whereas containerization doesn't need a hypervisor which saves the processor efficiency and improves its performance. And also, container size is flexible i.e., it can be changed dynamically, hence eliminates over-provisioning. Generally,
these virtual machines are installed as a form disk images, object, load balancers or IP addresses which can be dynamically installed on the cloud and also ensure the security of the virtual machine by allotting the virtual instance with a unique host address each time installed. These virtual instances are pre-installed on large pools of equipment called data centers. These virtual machines are billed by the service providers on the utility computing basis.

The general virtual components which can be offered by IaaS are-

1. Computer Hardware
2. Computer Networks (such as routers, firewalls, load balancers etc.)
3. Internet Connectivity (using optical carriers)
4. Platform virtualization environment for running client-specified virtual machines.
5. Service level agreements.

- **Advantages of IaaS are:**
  1. Readily available environment, customized for client, promotes efficient IT services.
  2. Maintenance such as software updates, latest versions can be readily available on the internet.
  3. Reduces the maintenance cost for the hardware which is quite expensive.

4. Data stored on the virtual machine is secured and can be recovered in case of any failure of host allocation.
5. Can accommodate many virtual instances as per the demand.
6. Virtual instances can be rented for machines like servers, operating systems, networks as a fully outsourced service.

Some of the IaaS service providers are:

1. Amazon Elastic Cloud Compute (EC2) service from Amazon Web Services by Amazon.
2. Google Compute Engine from Google Cloud Services by Google.
3. Windows Azure Virtual Machines from Windows Azure by Microsoft.
4. IBM Smart Cloud Enterprise by IBM.
5. HP Enterprise Converged Infrastructure from HP.

♦ **Disadvantages of IaaS are:**

1. Data security issues due to multitenant architecture.
2. Vendor outages make customers unable to access their data for a while.
3. The need for team training to learn how to manage new infrastructure [66].

2. Platform as a Service (PaaS)

Platform as a Service model focuses on providing platform and environment to the customers for creating services and applications using Internet. In the hierarchy architecture of service delivery model PaaS takes the middle layer, with SaaS layer above and IaaS layer below. The customers can ask for customized platform from the providers according to their requirements and pay-as-per the usage. Google App Engine is a well renowned working example for PaaS. The security issues due to multi-tenancy and data sharing has to be taken care by both the provider as well as the cloud user [26].

Dr. Chinthagunta Mukundha & K.Vidyamadhuri[25]: This service model delivers platforms for building and running web-based applications. It provides all the facilities required to support the complete software development life cycle. This service basically delivers a computing platform for the customer who includes operating system, programming platforms, web servers, databases etc. Since everything is run on internet, there is no need to worry about the infrastructure and minimum requirements for the platform. This model can hence eliminate the worry of incompatibility of software environment on the machine, since hardware specifications required by the platform are met by the cloud service provider directly,

thus providing powerful and unlimited computing power. Anyone with an internet connection can now develop powerful and efficient applications without worrying about the infrastructural and cost issues. The traditional on-premise models were expensive and complex, which required specific, set of hardware and software specifications. For every problem statement, there is a different business solution, which meant different set of hardware and software specifications. This situation used to force the developers to change the application every now and then. Enormous electricity power was also required to run the hardware. With the entry of PaaS model of cloud, application development became quick, cost effective and efficient. PaaS provides infrastructure along with the workflow facilities required for the software development. It also provides application services for the software development such as security, storage, database integration, instrumentation etc.

Another characteristic of PaaS model is the integration of web and mobile applications and services with the databases using Simple Object Access Protocol.

- **PaaS consists of three main components:**
  1. Stack- consisting of all the backend implementation components such as language virtual machine, servers, databases load balancers, caching mechanisms etc.
  2. Deployment Machinery- consisting of scripts and services for deploying the developed applications on the internet.
  3. User Experience- consisting of all the frontend components such as user interface, customized abstraction, flexibility to choose the environments and design.
- **2.2.3.2.2 Advantages of Paas are:**
  1. Can develop and deploy agile applications.
  2. Can focus on the important resources for the enterprise without worrying about the cost of infrastructure.
  3. The platforms provided by a PaaS provider are revised editions which are updated time to time, thus applications can be built using best technologies.
  4. Maximizes the productivity and minimized the development time.
  5. Doesn't require the developer to know the backend processes of the platform environment of the cloud.

  Some of the PaaS service providers are:

  1. Google App Engine by Google Cloud services from Google.

2. Windows Azure PaaS services by Windows Azure from Microsoft.
3. Amazon Elastic BeanStalk by Amazon Web Services from Amazon.
4. Openshift by Red Hat from Linux.
5. Engine Yard run on Amazon Web Services by Amazon [25].

♦ **Disadvantages of Paas are:**

1. Data security issues.
2. Compatibility of existing infrastructure (not every element can be cloud-enabled).
3. Dependency on vendor's speed, reliability and support [66].

3. Software as a Service (SaaS)

In the Software as a Service (SaaS) model, the client can access the provider's infrastructure through an interface. Most commonly used interfaces are web browsers. In this model a single instance on the service provider's end supports multiple access instants on the client's side. One main advantage of this model is that the consumer does not incur software licensing cost [27].

Dr. Chinthagunta Mukundha & K.Vidyamadhuri[25]: This service model provides the access to the application services and databases.

Cloud providers take care of the infrastructure and platforms required to run the software applications on the Internet. It is sometimes referred to as 'on-demand software', which can be used after paying the subscription fees. In this model, cloud users directly install the subscribed applications on the cloud and directly access the software from their cloud clients. The cloud users need not manage the necessary infrastructure or the platforms required to run the software application. Some of the SaaS applications are Customer Relationship Management (CRM), Enterprise Resource Planning (ERP), accounting and other business software, which are mainly non-core-competency software. Most of the companies today opt for SaaS solutions, which don't require the employee to know the infrastructure, background logics and platform details to run the application. Instead, he can just install the application on the cloud and run the application as a browser-based service on the Internet. The present day advancements in cloud make it easier for the customer to use these SaaS applications anywhere at any time. These applications can be used on a web browser

or a program interface without having to manage the specifications of the software. These applications have limited user-specific configuration settings which abstract most of the complex background details, making it easier for the user to deploy these applications.

- **Features of SaaS-**
  1. Can manage applications on a strong network and access to licensed software at low costs.
  2. Follows Multitenancy model.
  3. Customer specific enhancements of the software.
- **Advantages of SaaS are:**
  1. Easily available software reduces the time required for the application development.
  2. Increases the availability of the applications globally.
  3. Data consistency and compatibility across the company/organization/enterprise.
  4. These applications are scalable and flexible.
  5. The updated versions of the SaaS software are looked after by the service providers.
- **Disadvantages of SaaS are:**
  1. Loss of control
  2. Limited range of solutions
  3. Connectivity is a must [66].
- **Some of the SaaS service providers are:**
  1. Salesforce CRM from Salesforce.
  2. Oracle CRM from Oracle On-Demand from Oracle.
  3. SAP ERP and SAP CRM by SAP Business by Design from SAP.
  4. SaaS applications and services from Cloud9 Analytics [25].

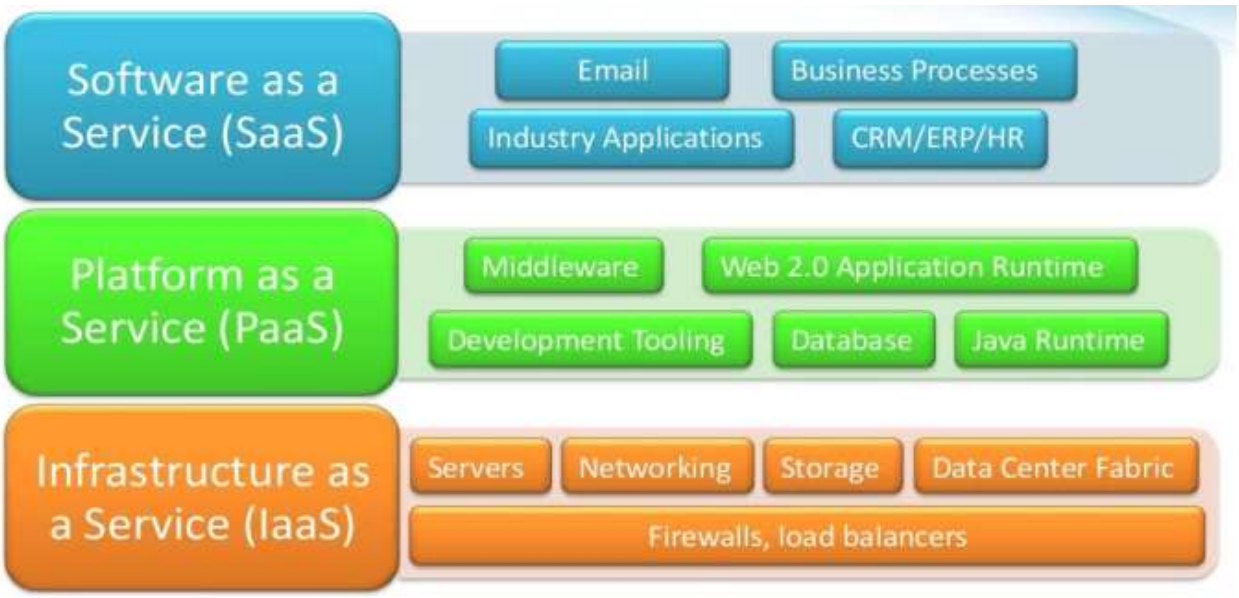


Fig 2.2- Cloud Service delivery Models and Services.

In our Project we going to deal with a Software as a service (Saas), In which our Case study we base on one at of it services.

2.3.4 Cloud Deployment models

NIST defines four cloud deployment models: **public clouds, private clouds, community clouds, and hybrid clouds.** A cloud deployment model is defined according to where the infrastructure for the deployment resides and who has control over that infrastructure. Deciding which deployment model, you will go with is one of the most important cloud deployment decisions you will make.

Each cloud deployment model satisfies different organizational needs, so it's important that you choose a model that will satisfy the needs of your organization. Perhaps even more important is the fact that each cloud deployment model has a different value proposition and different costs associated with it. Therefore, in many cases, your choice of a cloud deployment model may simply come down to money. In any case, to be able to make an informed decision, you need to be aware of the characteristics of each environment [28].

Selection of these models depends on clients' data sensitivity and management requirements [29].

These are the classification of Cloud deployment in details:

1. **Private cloud:**

Private cloud (internal cloud) infrastructure is dedicated to a single particular organization or group. It is not shared with other organizations. Private cloud can be owned or leased. It may be managed by the organization or a third party and can exist at on-premises or off-premises. Private cloud is more expensive and secure when compared to public cloud [30]. Private cloud is hosted inside the organization's firewall. It can be accessed by users within the organization via intranet as shown in figure 6 [31].

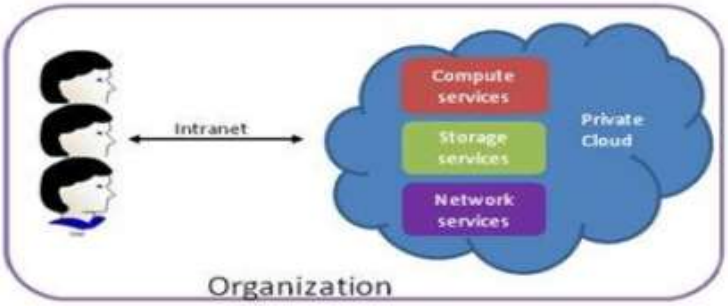


Fig 2.3- Private Cloud environment

Table 2.1: Highlight Pros and Cons of Private cloud

PROS	CONS
1. **Security and privacy.** Unlike public cloud models. 2. **Customization.** Compared to public cloud models, private clouds offer superior customization. 3. **Reliability.** While public cloud service plans can be scaled up or down fair easily.	1. It may come with a higher initial cost than other types of cloud deployment.

2. **Public cloud:**

Public cloud (external cloud) infrastructure is offered via web applications as well as web services over the internet to the public or a large industry group and is owned by an organization selling cloud services as shown in figure 7 [31].

Public cloud provides an elastic, cost-effective way to deploy IT solutions. The term public doesn't mean that users' data is publicly visible. Public cloud involves applications such as customer relationship management (CRM), messaging and office productivity [33]. Public cloud providers such as Google or Amazon offer an access control to their clients [32].

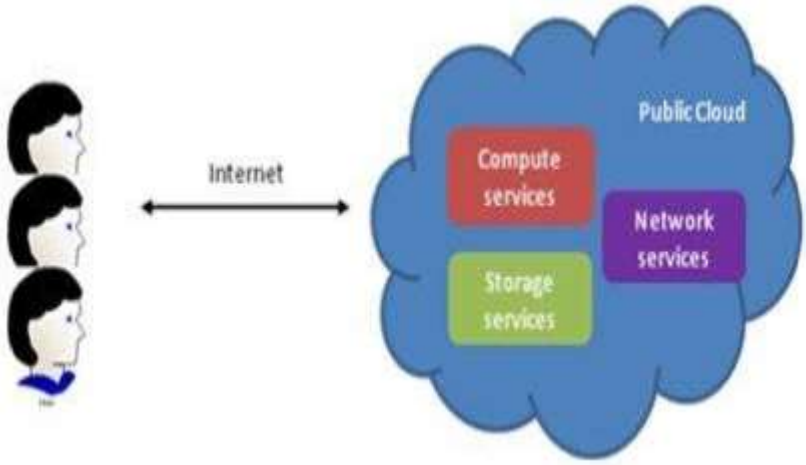


Fig 2.4- Public Cloud environment

Table 2.2: Highlight Pros and Cons of Public cloud

PROS	CONS
1. **Convenience.** The service provider is responsible for infrastructure setup and use, as well as the majority duties of organization.	1. **Potential security issues.** While users can easily access their own data, concerns remain regarding who else has access and where that particular data is kept.
2. **Reliability,** unlike on-site infrastructure owned by a small enterprise.	2. **Simplicity.** While simple service agreements are beneficial for many users, if not so, it may be difficult to find one to meet your needs.
3. **Scalability.** It allows you to easily scale your usage up or down as your needs require.	3. **Potential diminished reliability.**

3. Hybrid cloud:

This cloud deployment model exists due to mixed needs of an organization. It is combination of two or more cloud service deployment models (Private, Public, Community)

as shown in figure 8 [31]. Organizations may host critical applications on private clouds and applications with relatively less security concerns on the public cloud [32].

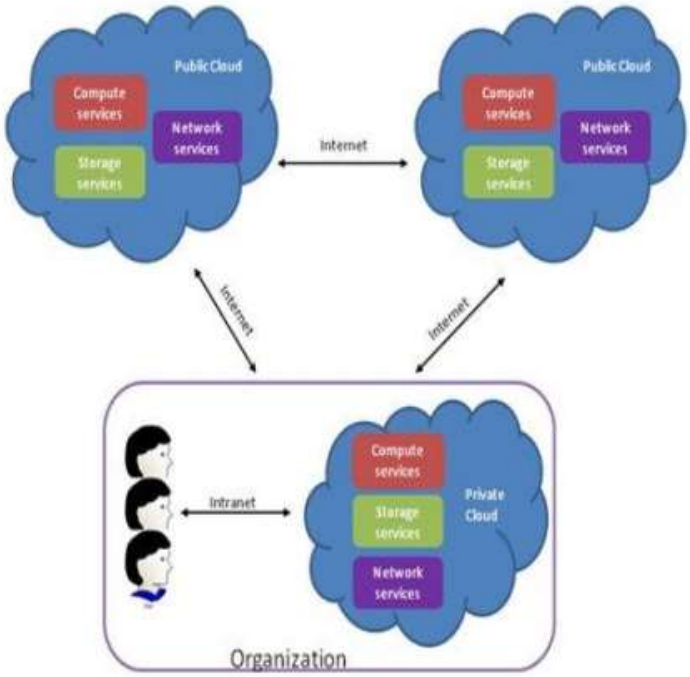


Fig 2.5- Hybrid Cloud environment

A combination of a public and a private cloud is joined together for the purpose of keeping business-critical data and services in their control on private cloud and outsourcing less-critical processing to the public cloud [34].

Table 2.3: Highlight Pros and Cons of Hybrid cloud

PROS	CONS
1. **Security and privacy.** Much like a private cloud.	1. Implementation can be complex and is usually best handled by a service partner with extensive experience in cloud deployments.
2. **Potential cost savings.**	
3. **Superior flexibility and scalability.** While both public and private cloud deployments are flexible and scalable in their own ways.	

4. Hybrid cloud:

Community cloud is a shared infrastructure by several organizations and supports a specific community that has shared concerns e.g., mission, security requirements, policy, and compliance considerations. It may be managed by the organizations or a third party and may

exist at on-premises or off-premises [35]. Community cloud offers higher level of privacy, security and policy compliances. Examples of community clouds include Google's "Gov Cloud".

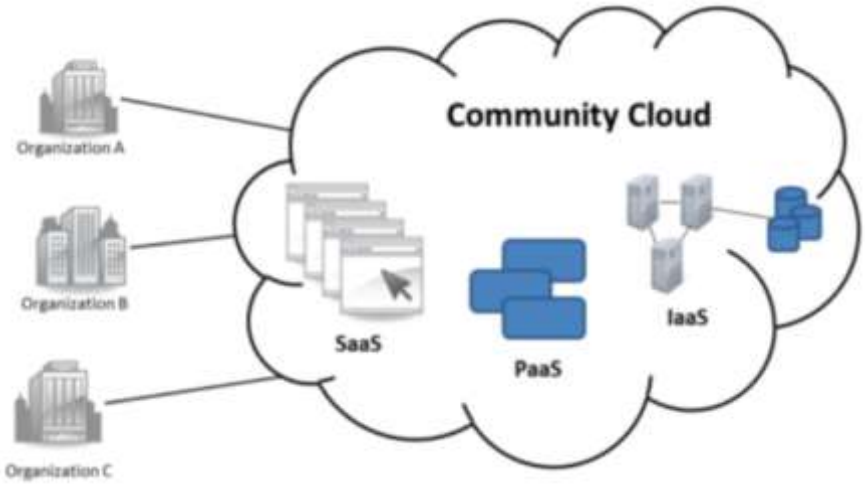


Fig 2.6- Community Cloud environment

Table 2.4: Highlight Pros and Cons of Community cloud

PROS	CONS
Cost Savings. Once established, you can pool resources with other organization and split the cost of maintenance and upkeep.	1. **Rarity.** It is still less common than other deployment models because it is necessary to locate other organizations with similar requirements.
Security and privacy. Similar to a private cloud deployment model with very limited access to user information.	2. **Relatively high cost.** Compared with other model, it has high initial cost.
Collaboration. With the availability of data sharing between organization on the community cloud, users can collaborate and undertake joint projects.	3.**Limited bandwidth and storage.** With multiple organizations sharing the same resources, bandwidth and storage capacity.

2.3.5 Benefits of Cloud computing:

Cloud Computing has numerous [36], benefits among these benefits are:

1. **Reduced Total Cost of Ownership**

The most widely touted advantages provided by Amazon EC2 are very similar to those offered by traditional outsourced data centers that offer reduced costs for hardware processing, storage, bandwidth and software. The major difference with EC2-like infrastructure clouds is that they are available to any size firm, from an individual backing up their music collection to a major retailer. Unlike complex data center service agreements, EC2 services are pay by use. Finally, they can be accessed easily through a small number of web services.

2. Increased Scalability and Reliability

It follows naturally that hosting the server side of your application in the cloud enables one to leverage the massive international infrastructure of the cloud provider.

This brings benefits of backup, reduced latency, fault tolerance and the ability to support peak demands. While many large corporations have such capabilities, far too many small businesses face constant challenges in this area so it isn't surprising to see SMB move to the cloud first.

3. Enabling Collaborative Applications

The ability to quickly build virtual business partnerships is a key competitive advantage. In a coopetition market place companies form multiple short-lived partnerships to exploit rapidly emerging business opportunities and specific niche markets.

4. Reduced Middleware Tax!

Despite the improvements in OO middleware by all vendors, it remains an unnecessary hardware and software tax that greatly complicates application development and deployment.

5. Increased Application Development Agility

Agile Development teams complain1 that they are blocked by downstream technology and policies with middleware, mainframe or application host operations, services and database units. Cloud Services and Databases provide increased flexibility for application focused teams to execute end to end. Cloud Services provide a simple but narrow API in which application developers have to live.

6. Increased End User Computing

The need to provide increasingly tailored solutions to meet the needs of end users and the costs of customized development naturally poses the question of whether more end user communities can support their own needs using some form of end user computing. JavaScript has become the Basic for the web and REST services the cloud API pattern of choice, both of which are consumable by end user developers.

2.3.6 Risks & Challenges of Cloud computing.

Security issues: Security risks of cloud computing have become the top concern in 2018 as 77% of respondents stated in the referred survey. For the longest time, the lack of resources/expertise was the number one voiced cloud challenge. In 2018 however, security inched ahead.

1. **Cost management and containment:** The next part of our cloud computing risks list involves costs. For the most part cloud computing can save businesses money. In the cloud, an organization can easily ramp up its processing capabilities without making large investments in new hardware. Businesses can instead access extra processing through pay-as-you-go models from public cloud providers.

   However, the on-demand and scalable nature of cloud computing services make it sometimes difficult to define and predict quantities and costs.

2. **Lack of resources/expertise:** One of the cloud challenges companies and enterprises are facing today is lack of resources and/or expertise. Organizations are increasingly placing more workloads in the cloud while cloud technologies continue to rapidly advance. Due to these factors, organizations are having a tough time keeping up with the tools. Also, the need for expertise continues to grow. These challenges can be minimized through additional training of IT and development staff.

3. **Governance/Control:** There are many challenges facing cloud computing and governance/control is in place number 4. Proper IT governance should ensure IT assets are implemented and used according to agreed-upon policies and procedures; ensure that these assets are properly controlled and maintained, and ensure that these assets are supporting your organization’s strategy and business goals.

4. **Compliance:** One of the risks of cloud computing is facing today is compliance. That is an issue for anyone using backup services or cloud storage. Every time a company moves data from the internal storage to a cloud, it is faced with being compliant with industry regulations and laws.

5. **Managing multiple clouds:** Challenges facing cloud computing haven’t just been concentrated in one, single cloud.

The state of multi-cloud has grown exponentially in recent years. Companies are shifting or combining public and private clouds and, as mentioned earlier, tech giants like Alibaba and Amazon are leading the way.

6. **Performance:** When a business moves to the cloud it becomes dependent on the service providers.
7. **Building a private cloud:** Although building a private cloud isn't a top priority for many organizations, for those who are likely to implement such a solution, it quickly becomes one of the main challenges facing cloud computing – private solutions should be carefully addressed.
8. **Segmented usage and adoption:** Most organizations did not have a robust cloud adoption strategy in place when they started to move to the cloud. Instead, ad-hoc strategies sprouted, fueled by several components. One of them was the speed of cloud adoption.

Migration: One of the main cloud computing industry challenges in recent years concentrates on migration. This is a process of moving an application to a cloud [37].

2.3.7 Factors affecting Cloud performance

There are several factors affecting the performance of cloud computing [38] among these factors are:

1. Network bandwidth: As the cloud is, a service provided online, when the bandwidth is low to provide a needed service at a required time this will cause a reduction in its performance.
2. Number of Users: When the number is users exceeds the cloud capacity, this could affect the performance of the service provided.
3. Data Recovery: The ability and time required to retrieve files affects the performance as data could be lost or subject to failures and this affects the performance.
4. Fault Tolerance: A high tolerance system will lead to high performance.
5. Other Factors: Other factors that can affect cloud performance include problems with scalability, latency, redundancy, workload, and processor power.[38]

2.3.8 Cloud computing reference architect

The NIST cloud computing reference architecture is a generic high-level conceptual model that is a powerful tool for discussing the requirements, structures, and operations of cloud

computing. The model is not tied to any specific vendor products, services, or reference implementation, nor does it define prescriptive solutions that inhibit innovation. It defines a set of actors, activities, and functions that can be used in the process of developing cloud computing architectures, and relates to a companion cloud computing taxonomy. It contains a set of views and descriptions that are the basis for discussing the characteristics, uses, and standards for cloud computing [39].

The NIST cloud computing reference architecture defines five major actors: cloud consumer, cloud provider, cloud auditor, cloud broker, and cloud carrier [39] as showing in the figure 2.7.

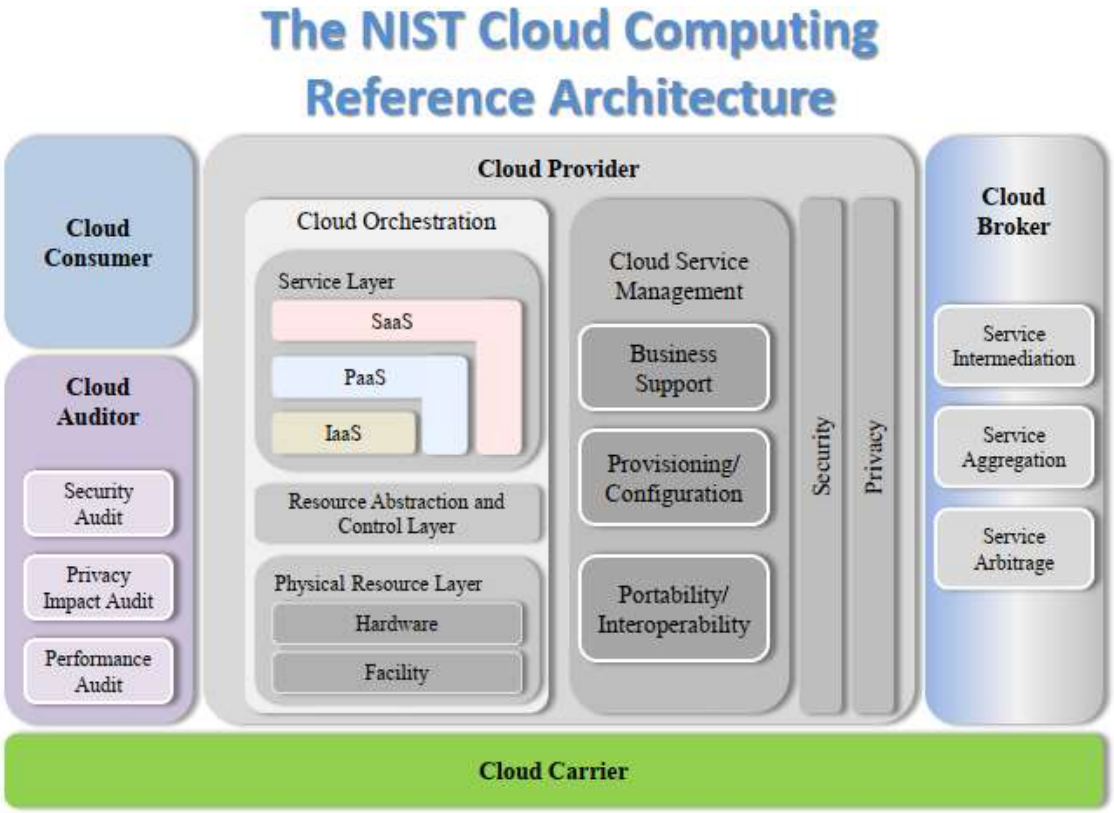


Fig 2.7- The NIST Cloud computing Architecture.

2.4 Security in Cloud computing.

Cloud security is a responsibility that is shared between the cloud provider and the customer. There are basically three categories of responsibilities in the Shared Responsibility Model: **(a) responsibilities that are always the provider's, (b)responsibilities that are always the customer's, and (c)responsibilities that vary depending on the service model:** Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS), such as cloud email.

The security responsibilities that are always the providers are related to the safeguarding of the infrastructure itself, as well as access to, patching, and configuration of the physical hosts and the physical network on which the compute instances run and the storage and other resources reside.

The security responsibilities that are always the customer's include managing users and their access privileges (identity and access management), the safeguarding of cloud accounts from unauthorized access, the encryption and protection of cloud-based data assets, and managing its security posture (compliance).

2.4.1 Cloud Security Issues and Threats

For us to get cleared about the vulnerabilities and threats in cloud we need to check one of the write up written by **Michael Novison** discussing about 12 Biggest Cloud threats and vulnerabilities in 2020, we need to follow as stated below [40]:

1. **Automated Attacks**

Automated attacks in the cloud have become easier and more popular as software gets less expensive, the quality of attacker builds improve, customers put more systems online and environments become more complex, according to Threat Stack's Bisbee.

The ability for any developer to put a system on the internet with just the swipe of a credit card has created an opportunity for highly leveraged automated attacks, Bisbee said. Software advancements have made large-scale data processing and collection easier for adversaries, Bisbee said, and there are often gaps between how a policy document said things work versus how everything is actually running.

2. **Low Barriers to Entry for Bad Actors**

The ubiquitous and available nature of compute and storage capabilities in the cloud has resulted in low barriers of entry for those looking to leverage cloud environments for malicious or nefarious efforts, according to Recorded Future's Solomon.

First off, Solomon said the cloud can be used as a launching point for attacks since it gives adversaries a relatively anonymous environment for organizing nefarious activity that can be easily set up or broken down. Second, bad actors can easily setup or stand down compute capability in the cloud, allowing it to host infrastructure or machine power for malicious activities from DDoS attacks to phishing campaigns.

3. **The Security Team Itself**

The traditional approach to secure directly conflicts with how the cloud is being used, and security teams can no longer expect to be the gatekeeper since departments can just go around them to get stuff done, said Mark Nunnikhoven, Trend Micro's vice president of cloud research. Security teams tend to be too worried about zero-day threats even though errors and misconfigurations cause more trouble.

Security teams often come across to other departments as arrogant or excessively focused on attacks, especially when there's no business context backing them up, Nunnikhoven said. And the security teams often find it easier to keep doing things the same way they've always done it since they're constantly in firefighting mode and feel like they don't have enough time to get their heads above water.

Security teams must become a trusted resource within their own organization by educating, training and informing other departments, Nunnikhoven said. They should also enable teams practicing a DevOps philosophy to move forward by delivering security in an automated fashion that checks for misconfigurations in a way that's compatible with how the team operates, according to Nunnikhoven.

4. **Excess Privileges**

Too many organizations fail to operate by the principle of least privilege in the cloud, making exceptions that result in too many people being granted administrator access to services and accounts, said Alert Logic's Dhamankar. Between 8 and 9 percent of Alert Logic's customer base has excess privileges on their accounts in areas like databases, which Dhamankar said can be a source of major trouble.

A lot of services in the cloud are interconnected, meaning that one exploited password could provide access across the entire cloud network if the administrative rights allow for that, said Alert Logic's Birk. As a result, Birk said a breach or attack on one individual account in the cloud could lead to exploit of greater magnitude.

Organizations must examine user behavior for irregularities as compared with other users in a similar role, Birk said. Companies should also consider what privileges the user had in the past and leverage machine learning to analyze what constitutes normal behavior for that particular user, according to Dhamankar.

5. **Infrastructure as Code Templates**

Developers are increasingly using templates they've found in places like GitHub as the basic building blocks for their cloud infrastructure, but putting these templates right into the cloud often introduces misconfigurations in the environment, according to Matt Chiodi, Palo Alto Networks' chief security officer of public cloud.

Given the massive number of cloud migrations happening, Chiodi said DevOps teams have begun using these templates over the past two years to build and scale quickly. Developers typically start by only using these templates in a dev environment, but they'll often end up in production environments with cloud storage logging disabled, meaning that potential security events can't be identified or attributed.

6. **Lack of Security Around Databases**

Too many organizations are leaving default database configurations in place as they rush to market with tools that might be in more of a prototype than production state, according to Tim Mackey, principal security strategist at Synopsys. As companies fight for market share in the cloud, many don't require third-party sign off on code changes and fail to examine deployments after the fact for any errors.

The database defaults or efforts to secure the instance by the person creating the database might not be sufficiently hardened, Mackey said. Companies therefore need either expertise on staff or through a channel partner around MongoDB, Microsoft SQL server and Oracle databases to ensure that all database instances have been identified and locked down, according to Mackey.

7. **Misconfiguration of Serverless, Container Environments**

Moving to serverless and containers environments has created a new perimeter and new types of workloads that organizations need to learn how to protect, according to Marina Segal, Check Point's head of product management for cloud SecOps and compliance.

Since serverless environments don't have underlying infrastructure, Segal said companies must ensure the function itself has the right set of definitions and policies in place that won't allow for the execution of malicious activities. There must also be a presence in run time to analyze the behavior of functions and block anything that's abnormal, according to Segal.

If unencrypted keys are left as plain text in a user's code and that code ends up in a public repository or getting exposed, Segal said attackers can leverage those keys to get to many other places in the company's environment. Businesses should leverage a cloud-native key management system and make sure keys are encrypted and rotated instead of leaving them in plain text as part of the code, Segal said.

8. Breakdown in Shared Responsibility Model

Adversaries are taking advantage of a breakdown in the shared responsibility model as it relates to the data access rights and data standards, according to Stu Solomon, Recorded Future's chief operating officer. In a traditional structured environment, he said users are granted access to data based on their job role or responsibility and the administrator can monitor, maintain, control or manage their access.

And when migrating into a cloud environment, Solomon said data identification, data classification and a constant review and reconfirmation of an individual's need to access that data must continue. The monitoring and enforcement of individual access rights can sometimes be overlooked during the migration process itself, according to Solomon.

Migrations are typically initiated and executed outside the security team by business and operational decision-makers, and security practitioners are often now involved in the process whatsoever, Solomon said. As a result, Solomon said data access issues can crop up once the migration is complete and day-to-day operations have returned to a normal basis.

9. Lack of Adherence to Policies

Organizations will often write cloud security policies in a document and hand it over to the DevOps team without addressing thoroughly considering how these policies will be put in place, according to Steve Quane, Trend Micro's executive vice president of network defense and hybrid cloud security.

Security teams expect someone else in the organization to configure and implement the cloud security policies, while DevOps teams don't do manual configuration or implementation and expect a Terraform script or something automated, Quane said. Account information is needed to pull up APIs, but given that most organizations have a bunch of different account owners, it isn't clear who to ask, Quane said.

10.Interconnectivity of Cloud Functions

Many organizations don't understand the basics of how to configure and harden cloud technologies as well as how cloud services interact with one another, according to Sam Bisbee, chief security officer at Threat Stack. Virtual machines are increasingly considered users in the context of a cloud environment and are therefore leveraging APIs from public cloud vendors to request keys and change infrastructure.

Therefore, if an organization has a compromise, Bisbee said the attacker can make a network call and start controlling the infrastructure. The interplay between networked services is something that most teams aren't prepared to deal with, according to Bisbee.

11.Lack of Continuous Scanning

Clients often aren't aware of new items in their environment since applications are constantly getting spun up and down, and rapid deployment could lead to the rapid introduction of problems, according to Onkar Birk, Alert Logic's chief product officer.

The ease with which apps can be introduced into an environment has made it difficult for companies to detect and orchestrate security around them, Birk said. Clients often have a multitude of departments spinning up cloud applications, and Birk said it's difficult for companies to centrally manage that if they aren't fully aware of what's going on.

12.Multitude of Configuration Options

Organizations can navigate the shared responsibility model successfully if they use products and integrations properly, which really comes down to customer education, according to Matt Pley, Fortinet's vice president of cloud and service providers.

Configurations are the most common source of errors given the number of mechanisms and things users need to know inside the cloud, Pley said. Getting a guided tour through the configuration is so important when building out cloud applications and infrastructure, according to Pley [40].

2.4.2 Cloud Security Goals

The CIA Triad refers to the 3 goals of cyber security Confidentiality, Integrity, and Availability of the organizations systems, network and data [41]:

1. **Confidentiality** – Keeping sensitive information private. Encryption services can protect your data at rest or in transit and prevent unauthorized access to protected data.

2. **Integrity** – is the consistency of data, networks, and systems. This includes mitigation and proactive measures to restrict unapproved changes, while also having the ability to recover data that has been lost or compromised.
3. **Availability** – refers to authorized users that can freely access the systems, networks, and data needed to perform their daily tasks. Resolving hardware and software conflicts, along with regular maintenance is crucial to keep systems up and available.

We can extend the definition by categorize the following point among the cloud goals:

4. **Authenticity**: proves that all parties involved in an action are who they claim to be by validating their identities. In information security, Message Authentication Codes (MAC) or digital signatures are used to ensure the authenticity of data, transactions, communications or, documents, i.e., that the information is genuine and authentic [42].
5. **Non-Repudiation:** In information technology and communications, non-repudiation assures that a sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data. In electronic commerce, digital signatures are used to establish authenticity and non-repudiation [42].

2.4.3 Confidentiality in Cloud computing.

Confidentiality ensures that data which is there in the cloud can be accessed only by the authorized party. This way the cloud service provider can guarantee the user that his data does not get into the wrong hands and also increases the user's trust in cloud computing and help it grow further.

Moreover, if the cloud server user has control over his data, it would further increase the security. Security is an important aspect of cloud computing due to a greater number of parties, devices and applications involved and because of this the threat of compromise of data is high. This happens because of the increase in point of access. Since confidentiality plays a major role in protecting organizational or individual data, information security protocols should be implemented at various different layers of cloud applications. There is always a possibility that the data stored in the cloud may mingle with other user's data. Data can also be compromised

unintentionally due to data remanence. It is the residual representation of the data that remains even after efforts are made to erase the data. Confidentiality can also be compromised due to non-trustworthy cloud service providers (CSP). Confidentiality can be ensured through better encryption techniques. Basically, there are two different approaches to achieve confidentiality: physical isolation and cryptography [43].

2.4.4. Some Techniques to Enhance Confidentiality

A. Biometric encryption (BE)

Confidentiality of biometric data can be achieved through biometric encryption. Biometric identification includes iris, voice, fingerprint, face recognition etc. Biometric identification has shortcomings. Some have been hacked using fake biometric information attack, such as fake fingerprints attacks. Biometric encryption is a technique that has been used to protect biometric identification. Biometric encryption is different from normal password encryption because here the biometric image is merged with the randomly generated key using BE binding algorithm to create biometrically encrypted key [44].

B. Secret Sharing Scheme

This scheme is used with public private hybrid cloud storage approach. This is achieved by developing a secure and fully automated data storage and transfer protocol in cloud between cloud storage providers and consumers. Here it is assumed that the cloud consumer has access to multiple storage volumes on the cloud side in order to save its data. In this approach the sensitive data is secured in the private cloud infrastructure before sending it to public cloud for storing. This protocol is implemented in two phases with a secret sharing scheme. The send phase occurs when a file is being stored or updated in the public cloud storage and the retrieve phase occurs when a file is being accessed or downloaded from the cloud infrastructure [45].

C. Confidentiality preserving through encryption and obfuscation

Normally confidentiality is achieved through encryption. But encryption alone may not provide security. This technique uses both encryption and obfuscation to preserve the confidentiality as it considers encryption alone cannot provide security. Same with the case of obfuscation as reverse engineering attacks or brute force techniques can break this.

Here obfuscation is integrated with encryption. Obfuscation uses a mathematical function or employs programming techniques to disguise illegal users. This approach depends on the type of data. Encryption can be applied to alphabets and alphanumeric type of data and obfuscation to numeric data [46].

D. K-NN classifier for data confidentiality

This approach classifies the data to be stored based on their security needs, like what data need security and what data do not need security. This is done using K-NN classification scheme. Data is classified into two classes, sensitive and non-sensitive. RSA algorithm is applied to the sensitive data whereas non sensitive data is stored as it is. KNN machine learning technique is used to separate the sensitive data from non-sensitive data. K-NN is used in a designed simulation environment. For accuracy purpose, the value of k is maintained to one (1). After separating sensitive from non-sensitive data, sensitive data is passed to RSA algorithm for encryption. Non sensitive data is directly allocated a Virtual Machine without encryption. Sensitive data is that data which is very important for individual or organizations like personal data, financial records, business material, legal, medical, government data etc. Non sensitive data are those which can be made public like announcements, marketing information etc. The K-NN is a supervised machine learning technique. It depends on instance-based learning, where to classify new unclassified data sets into user specified classes 'k', a set of training data is stored. K-NN calculates the distance between new input and all of training data and then sorts the distance to determine the Kth minimum distance.

Finally, it determines the class of the new input based on the majority vote. The cloudsim simulator is used for simulation purpose. Virtual Machine Manager is used to manage and assign VMs to cloud tasks [47].

2.4.5 Cloud Security Existing solution and mechanism.

As it previously discussed that one of the issues affecting the cloud-computing environment is the issue of security, Cloud users implement various mechanism and technique for maintaining security, researchers have proposed various solutions too, in this thesis we interested in the following mechanism: **Authentication mechanisms, Authorization mechanism, Encryption Mechanism, Access Control mechanism.**

1. **Authentication mechanism:** Authentication is the process of ensuring that the right entity is accessing the data. In cloud authentication refers to making sure that the user is storing the data by giving a valid user name and password which is a single factor authentication method employed. The user has to prove his/her identity to the cloud service provider to

access the various data stored in the cloud. RSA [48] considers that the private and public cloud has different authentication schemes. A single login using trust policies and strong authentication methods are used.

It has proposed a centralized virtualization management console which is used to safeguard the private clouds from unauthorized access. Some of the authentication schemes adopted by the RSA includes knowledge-based authentication, two factor authentication and adaptive authentication. Reduced cost and improved security are provided.

2. **Authorization mechanism:** Authorization ensures that the user submits its user identity in order to login to a particular service. This method is the step followed after authentication. Oracle [49] has proposed an Oracle Database Vault which protects the application data from various administrative users and also provides authorization. An access control mechanism based on Role Based Access [50] was proposed for multi-tenancy method of protecting the data in cloud environments. The segregation of duties of various administrators is provided such that an administrator in a particular domain will not be able to access the other domain.

A policy-based authorization scheme [51] which can be run as an Infrastructure as a Service model in order to protect the user's privacy by ensuring that they can set their own privacy policies in order to protect the user data from unauthorized access.

3. **Encryption mechanism:** Encryption is the process of making plaintext in to an unreadable format by a user or a third party. The conversion is made in to cipher text which has to be decrypted at the receiving side. The data is encrypted before it is stored in to the cloud to ensure that the cloud service providers does not read or modify the data contents stored in the cloud. The cloud service provider may either sell the data or view the contents by violating the security of the user.

Dell [52] data protection/encryption has allowed for protecting the various user data that

is being stored on an external drive or media. Software and hardware-based encryption schemes are deployed. The main advantage being that the user intervention is not required to enforce policies and they are easy to deploy and manage as well. Dell also has employed the Transparent File Encryption in which a control over the various users accessing the data is maintained. In this method a white list of users are created who will be given the access to services and to share files. The monitoring of the usage, auditing of events and report creation and the workload of the compliance is also reduced.

4. **Access control:** is the method of ensuring that the access is provided only to the authorized users and hence the data is stored in a secure manner. Various access control mechanisms such as firewall, Intrusion detection and segregation of duties are enabled at various layers of the network and cloud. Various access control Lists (ACL) are created in which users are classified as white list and black list for separating and providing access based on a Defence in Depth method. The firewall is deployed in the network to allow only the filtered contents to pass through which can be set up by the users based on a certain set of policies. The Demilitarized zone is put in to the firewall wherein, it provides an extra layer of security and make sure that the data is safe [53].

2.5 Overview on man-in-cloud Attack.

2.5.1 man-in-cloud attack:

MITC attacks allow cybercriminals to access data and documents stored in popular file synchronization services such as Google drive.

MITC attacks are also incredibly difficult to detect even with cutting-edge cybersecurity systems, the report surmised. Hackers do not need the internet, and they can infiltrate accounts by simply altering registry keys, so users won't be aware of the breach either. To further heighten the severity of MITC attacks, Imperva researchers wrote that once Google Drive accounts are compromised via a MITC attack, they must be deleted them for good, as there is no way to remove the threat [54].

MitM attack is a type of attack carried out by a malicious internal user on two computers by pretending to one that he is the other [55]. MitM can be of two categories [56]: **Eavesdropping** and **Manipulation**. **Eavesdropping:** is passive as the adversary is only

interested in the information passing through. In **Manipulation** MitM, the adversary changes data while masquerading it as the original sender.

2.5.2 How to detect and prevent from man-in-the cloud attacks

The nature of the MitC attack makes it very difficult to prevent with conventional security measures such as endpoint and perimeter protection. However, there are several steps that organizations can take to significantly minimize (or even eliminate) the chance of becoming a MitC victim [57].

1. **Conduct regular security training** – One of the most effective security measures is also one of the simplest. As mentioned above, MitC attacks rely on social engineering to be successful. Fortunately, a well-trained, vigilant employee is far less likely to click on a malicious link or a suspect attachment inside of a phishing email. Security-conscious organizations should conduct regular trainings with all of their employees in order to keep security top of mind and ensure that they know the tell-tale signs of an attempted attack.

2. **Use encryption to protect cloud data** – While encryption cannot prevent an MitC attack from occurring, it can prevent the data breaches that may take place as a result. Provided the encryption keys are not also stored within the targeted cloud service, any data accessed through an MitC attack would remain encrypted to the attacker. This means that the stolen information would be indecipherable and unusable to the malicious party.

3. **Enable two-factor authentication** – multi-factor authentication (MFA), is another simple but effective way to help minimize the threat of MitC attacks. This authentication capability is available with leading cloud services (Office 365) as well as from specialized security solutions built to verify users' identities across all of an organization's cloud-based resources. MFA adds an extra layer of security that can easily thwart an MitC attacker who doesn't have the ability to authenticate beyond an OAuth token.

4. **Invest in a cloud access security broker (CASB)** – One of the most comprehensive ways to protect against threats like MitC attacks is through the deployment of a CASB. CASBs intermediate all traffic between an organization's cloud apps and endpoint devices – they automatically replace each app's OAuth tokens with encrypted tokens before delivering them to endpoints. As a device attempts to access a cloud app, the unique, encrypted token is presented to the CASB, which decrypts it and passes it along it to the app. Consequently, if a user's token were to be replaced with a hacker, then the malicious token would fail validation and decryption at the proxy, denying access to the intended victim's account and nullifying the attack [57].

2.6 Cryptography Overview

2.6.1 Cryptography.

Cryptography is the process of writing the secret information in human unreadable secret format. Encrypt the plaintext into the cipher text by using the secret key which cannot be

readable by an unauthorized person and transfer the cipher text between the parties on an insecure channel. After the data is received at the receiver side the cipher text is decrypted using the valid secret key and retrieves the original message. Without the knowledge of a secret key, the attacker cannot retrieve the secret message. Cryptography is used for secure communication across the insecure channel like **privacy, confidentiality, non-repudiation, and authentication [58].** Figure 10 below showing how encryption works;

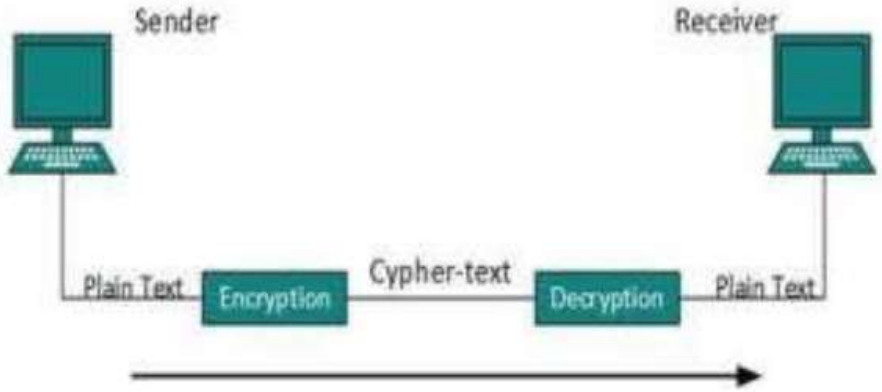


Fig 2.8 - Cryptography Architecture.

2.6.2 Popular Encryption system.

These are different techniques use to encrypt data or information in transmission channel in order not to attack by the middle man [59]:

1. **Advanced Encryption Standard (AES)**

AES is the most popular and broadly used symmetric encryption standard today. Due to the DES's small key size and low computing capability, a replacement was required which led to the development of AES.

Compared with TripleDES, it has been proved to be more than six times faster.

It is seen while using messaging applications such as Signal and Whatsapp, computer platforms such as VeraCrypt and other technologies commonly used.

The AES standard constitutes 3 block ciphers where each block cipher uses cryptographic keys to perform data encryption and decryption in a 128-bit block.

A single key is used for encryption and decryption thus both the sender and receiver have the same key.

The sizes of the keys are considered adequate to secure the classified data to a satisfactory secret level.

2. **IDEA encryption algorithm**

The international data encryption algorithm abbreviated as IDEA is a symmetric block cipher data encryption protocol.

The key size of the block cipher is 128 bits and is regarded as a substantially secure and one of the best public standards.

Typically, the block cipher runs in round blocks. It applies fifty-two subkeys where each has a 16-bit length.

Two subkeys are applied for a single round, four subkeys are applied prior to and after every round. Typically, both the plain text and the ciphertext have equal sizes of 16 bytes.

3. **MD5 Encryption Algorithm**

This protocol was purposely developed to offer data security as it can take inputs of arbitrary size to generate a 128-bit hash value output.

Under this protocol, the encryption technique follows 5 phases where every phase features a predefined task.

The five steps include:

-Append padding (adding additional bits to the input) bits

-Append the length -Initializing MD buffer -Message processing

-Output

One notable advantage of MD5 is that the protocol allows the generation of a message digest using the initial message. Nevertheless, the protocol is relatively slow.

4. **HMAC encryption algorithm**

HMAC stands for hash message authentication code and it is applied to ascertain the message integrity and authenticity.

The protocol applies 2 hash computation passes and a cryptographic key.

This standard resembles most digital signatures only those symmetric keys are used in HMAC whereas asymmetric types of keys are used in digital signatures.

5. **RSA Security**

This standard offers protection against cyber-attacks by detecting and responding to threats, preventing online fraud, management identification, et al. Its data encryption is founded on the

application of both a public key as well as a private key. RSA algorithm generates the two keys simultaneously.

When the computer is running on a secure website, the protocol generates a public key that is available publicly for data encryption.

On the other hand, the encrypted text is decrypted using the private key. Sender identification is done with the aid of the public key [59].

2.6.3 AES algorithm Overview.

The Advanced Encryption Standard (AES) algorithm is a symmetric block cipher that processes image which is of blocks size 128 bits using three different cipher key size of lengths 128,192 or 256 bits. Based on the key size length used, the number of execution rounds of the algorithm is 10, 12 or 14 respectively [68]. We need to explain more features about AES algorithm which it as follow:

I. Evaluation criteria for AES algorithms

Three important criterions were used by NIST to evaluate the algorithms that were submitted by cryptographer experts.

A. Security

One of the most crucial aspects that NIST was considered to choose algorithm it is security. The main reasons behind this were obvious because of the main aims of AES was to improve the security issue of DES algorithm. AES has the best ability to protect sensitive data from attackers and is not allowed them to break the encrypt data as compared to another proposed algorithm. This was achieved by doing a lot of testing on AES against theoretical and practical attacks [69].

B. Cost

Another criterion that was emphasis by NIST to evaluate the algorithms it is cost. Again, the factors behind these measures were also clear due to another main purpose of AES algorithm was to improve the low performance of DES. AES was one of the algorithms which was nominated by NIST because it is able to have high computational efficiency and can be used in a wide range of applications especially in broadband links with a high speed [70].

C. Algorithms and implementation characteristics

This criterion was very significant to estimate the algorithms that were received from cryptographer experts. Some important aspects were measured in this stage that is the

flexibility, simplicity and suitability of the algorithm for diversity of hardware and software implementation [71].

II. Basic Structure of AES algorithm

AES is an iterative instead of Feistel cipher. It is based on two common techniques to encrypt and decrypt data knowns as substitution and permutation network (SPN). SPN is a number of mathematical operations that are carried out in block cipher algorithms [72]. AES has the ability to deal with 128 bits (16 bytes) as a fixed plaintext block size. These 16 bytes are represented in 4x4 matrix and AES operates on a matrix of bytes. In addition, another crucial feature in AES is number of rounds. The number of rounds is relied on the length of key. There are three different key sizes are used by AES algorithm to encrypt and decrypt data such as (128, 192 or 256 bits). The key sizes decide to the number of rounds such as AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys [73].

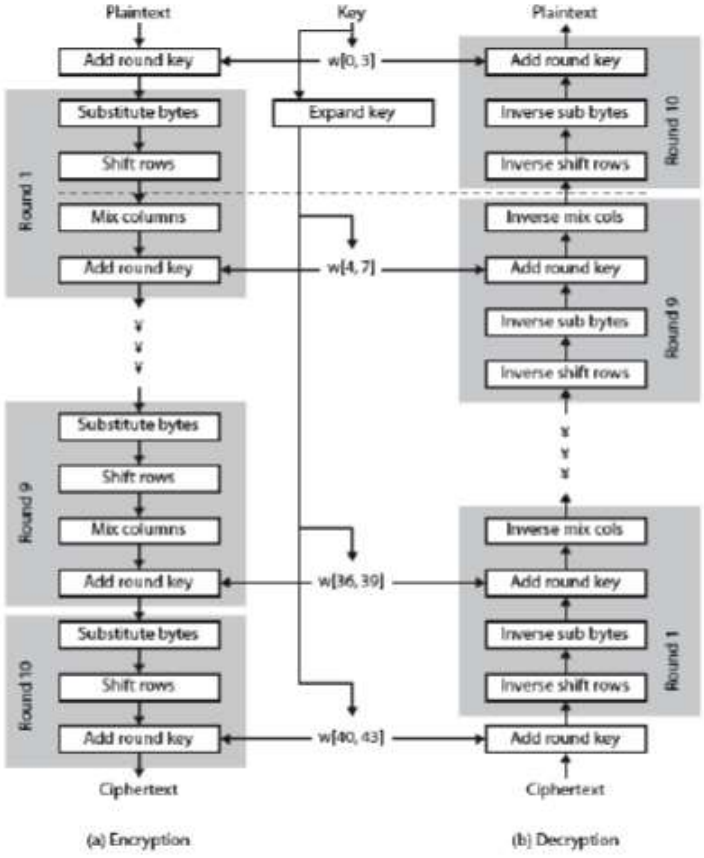


Fig 2.9 – Basic Structure of AES algorithm.

III. Encryption process.

Encryption is a popular technique that plays a major role to protect data from intruders. AES algorithm uses a particular structure to encrypt data to provide the best security. To do that it relies on a number of rounds and inside each round comprise of four sub-processes. Each round consists of the following four steps to encrypt 128-bit block

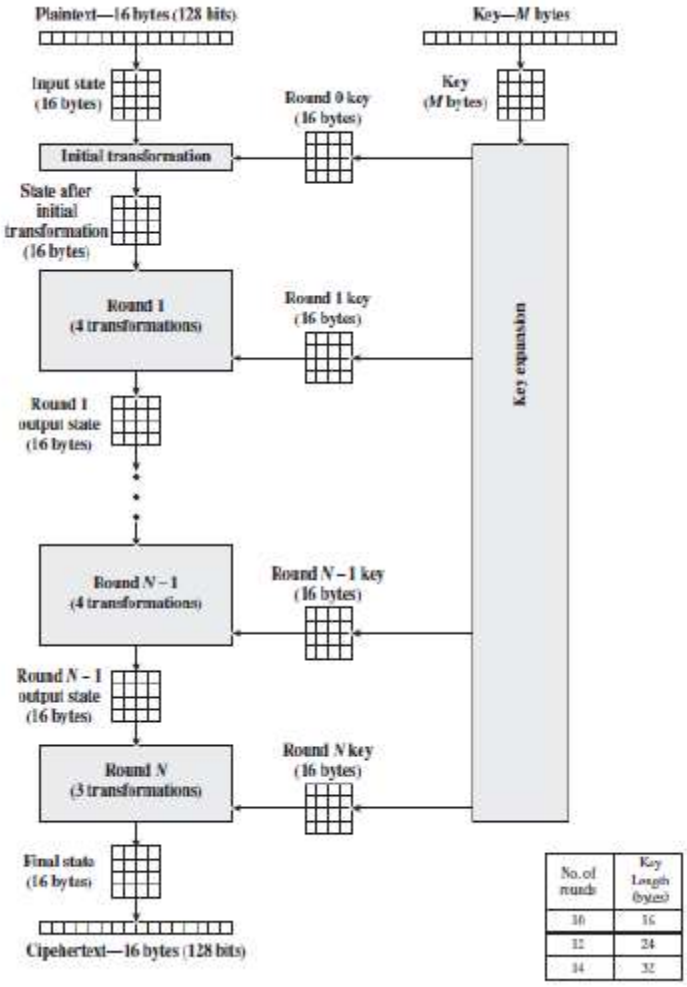


Fig 2.10 – Encryption process.

2.7 Steganography Overview

2.7.1 Steganography:

is a technique whereby we put the existence of a message to question by simply covering it up within another file image or video. Steganography is derived from the Greek words staganos and graphein, meaning “covered, concealed, or protected” and “writing,” respectively. Steganography differs from cryptography in that cryptography simply encrypts the intended message, whereas steganography keeps the existence of the message a secret: that is, cryptography conceals the contents of the message, whereas steganography conceals the

existence of the message. Steganography conceals information within computer files and media files, being the most eligible candidates. In steganography, mostly least significant bits are replaced with the message bits and they are imperceptible to the human eye. For example, consider embedding data in alternate pixels of a picture. The results show subtle changes that would not be noticed by a person who sees it as a picture only. The main factor which is of concern during transfer of data, i.e., data communication, is the security of the data. Data scrambling (encryption) and steganography have come into the limelight because of simplicity in implementation. A combination of both would suffice for the intended requirements – with security being primary, amount of data that can be embedded secondary, etc[60].

2.7.2 Types of steganography:

We have different type of media using to hide message in cyber-security, but these are commonly used media mentioned below [61]:

Text steganography: It consists of embedding the message inside the text file. The text steganography requires low memory. Various methods are available for hiding information in a text file. The methods are the random and statistical method, format-based method and linguistic method.

Image steganography: It consists of embedding the message inside the pixel of the image. The hacker cannot identify the original message. **LSB is a commonly used algorithm in image steganography.**

Audio steganography: It consists of embedding the message inside the audio files. Audio steganography hides the information in AU, WAV and MP3, and sound files. There are various methods available in audio steganography. The methods are spread spectrum, low bit encoding, and phase coding.

Video steganography: It is the process of hiding the secret information inside the digital video format. Some format is used for video steganography are Mp4, MPEG, AVI [61].

2.7.3 Techniques Using in steganography:

We need to discuss little at of techniques using in steganography for hiding secret message, they are as following [62]:

1. **Spatial Domain Methods:** spatial domain Steganography technique refers to methods in which data hiding is performed directly on the pixel value of cover image in such a way

that the effect of message is not visible on the cover image. The spatial domain methods are classified as following:

a. **LSB:** LSB is one the technique of spatial domain methods. LSB is the simple but susceptible to lossy compression and image manipulations. Some bits are change directly in the image pixel values in hiding the data. Changes in the value of the LSB are imperceptible for human eyes. Eg:

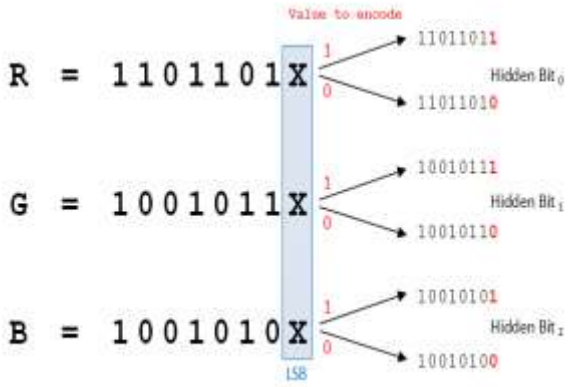


Fig 2.11 – Example of LSB conversion.

We are going to use this technique in our proposed method.

b. **Pixel Value Differencing:** To embedding the data in PVD the two consecutive pixels are selected. Whether the pixels are determining from smooth area or an edge area. Payload is determined by calculating the difference between two regular pixels.

c. **BPC:** The Binary Pattern complexity approach is used to measure the noise factor in the image complexity. The noisy portion is replaced by binary Pattern and it is mapped from the secret data. The image will remain same when the reverse noise factor will be determined [62].

2. **Transform Domain Steganography:** It is a more complex way to hides the information in an image. The different algorithms and transformations are used to hide information in the images. In the frequency domain, the process of embedding data of a signal is much stronger than embedding principles that operate in the time domain. The transform domain techniques over the spatial domain techniques is to hides the information in the images that are less exposed to compression, image processing and cropping. Some transform domain techniques are not depending on the image format and they run the lossless and lossy format conversions. Transform domain techniques are classified into various categories such as

Discrete Fourier transformation (DFT), discrete cosine transformation (DCT), Discrete Wavelet transformation (DWT)[62].

3. **Vector Embedding:** A vector embedding method that uses robust algorithm with codec standard (MPEG-1 and MPEG -2). This method embeds audio information to pixels of frames in host video. It is based on the H.264/AVC Video coding standard. The algorithm designed a motion vector component feature to control embedding, and also to be the secret carrier. The information embedded will not significantly affect the video sequence's visual invisibility and statistical invisibility. The algorithm has a large embedding capacity with high carrier utilization, and can be implementing fast and effectively [63].

2.7.4 LSB algorithm Overview

Least Significant Bit Replacement Technique: In image steganography almost all data hiding techniques try to alter insignificant information in the cover image. Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image. For instance, a simple scheme proposed, is to place the embedding data at the least significant bit (LSB) of each pixel in the cover image [74,75,76]. The altered image is called **stego-image**. Altering LSB doesn't change the quality of image to human perception but this scheme is sensitive a variety of image processing attacks like compression, cropping etc.

THE LSB TECHNIQUES

The least significant bit i.e., the eighth bit inside an image is changed to a bit of the secret message. When using a 24- bit image, one can store 3 bits in each pixel by changing a bit of each of the red, green and blue colour components, since they are each represented by a byte. An 800×600-pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. As an example, suppose that we have three adjacent pixels (9 bytes) with the RGB encoding.

10010101 00001101 11001001
10010110 00001111 11001011
10011111 00010000 11001011

When the number 300, can be which binary representation is 100101100 embedded into the least significant bits of this part of the image. If we overlay these 9 bits over the LSB of the 9 bytes above, we get the following (where bits in bold have been changed)

10010101 00001100 11001000

10010111 00001110 11001011

10011111 00010000 11001010

Here the number 300 was embedded into the grid, only the 5 bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size. Since there are 256 possible intensities of each primary colour, changing the LSB of a pixel result in small changes in the intensity of the colours. The human eye cannot perceive these changes - thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the LSB without noticing the difference [77].

2.8 Related works.

These are different kind of papers, which has relevant or similar to our project:

2.8.1 First study

The study of Dheyab Salman Ibrahim **2019** [13], **Enhancing Cloud Computing Security using Cryptography & Steganography,** Paper, Iraqi Journal of Information Technology. V.9 N.3.

The large challenge of data stored in “cloud computing” is confidence and security since the sensitive data saved into data centers in cloud. These critical data may be accessed, retrieved, or edited by unauthorized person(s) or machine(s). In addition, managing, organization of sensitive data may not be secure. Therefore, the security of data is highly interesting. To increase the security of data in data centers of cloud, they introduced scheme to ensure data security in “cloud computing” by encoding secret data using two levels of encryption are DES & RSA algorithms. And then to enhancing the security we use LSB algorithm to hide these encrypted data inside edges of color images which is called steganography.

The fundamental objective of this paper is to avoid data access by opponent users.

Result analysis contain security analysis. The security analysis consists of analyzing several security characteristics such as:

1. Data Confidentiality- is analysed by comparing it with another data encrypted by DES, AES which uses the one key to encrypt/decrypt data. Use RSA only, or LSB. In our proposed system, do not have any access to personal data in cloud, doe employed three levels of security. The one knows the key for three algorithms and is only know to the data owner which ensures the data confidentiality.
2. Authentication – is performed with help of the password set by the user through registration.
3. Integrity – ensures that data integrity into the cloud.
4. Hybrid method made the encryption and decryption process stronger.
5. RSA and DES are used as an integrated approach where data was encrypted with DES and private key can be encrypted with RSA algorithm. This leads to increase in performance compared with other techniques.
6. The combination of symmetric and asymmetric encryption techniques (such as DES and RSA) leads to ensure the security in the cloud computing.

We will try to propose another Steganography algorithms which is more powerful in performance than LSB algorithm.

2.8.2 Second Study

The study of Vipula Madhukar Wajgade and Dr. Suresh Kumar **2013** [14], **Enhancing Data Security Using Video Steganography,** Paper, International Journal of Emerging Technology and Advanced Engineering, Volume 3.

Information security has become the area of concern as a result of widespread use of communication medium over the internet.

This paper focuses on the data security approach when combined with encryption and steganographic techniques for secret communication by hiding it inside the multimedia files.

Where they used AES for encryption and SHA-1 for generating secret hash function or key.

Which results in more secure technique for data hiding. They concluded that the proposed system is more effective for secret communication over the network channel.

The drawback of this research is that: there is no specified Steganography algorithm to work with, and that means security level is low.

My Opinion is to substitute hash function algorithm with steganography algorithms in order to make the performance more reliable and standard.

2.8.3 Third study

The study of R SHANTHAKUMARI and S MALIGA **2019** [15], **Dual-layer security of image steganography based on IDEA and LSBG algorithm in the cloud environment,** Paper, Sadhana journal (2019).

The architecture development of cloud computing technology is growing tremendously in recent times, which leads to improvement of scalability, accessibility and cost reduction measures in the IT sectors of all enterprises. In this service, the data storage without reviewing security policies and procedures is a challenging task and probabilities of extracting secret information by an unauthorized intervention are more.

However, to prevent the breaches of security in the cloud service, the steganography art plays an essential role in the data communication medium to improve the security measures, and it is an indispensable technique for hiding the secret information into a cover object. This paper describes the implementation of new steganography method with International Data

Encryption Standard Algorithm (IDEA) and Least Significant Bit Grouping (LSBG) algorithm for embedding the secret information into an original image and extracting the same. The result shows the improvement of data embedding capacity and reduces the issues related to data security by effective utilization of this new approach, which reveals the remarkable achievement of the combinational execution of steganography and cryptography technique. The IDEA and LSBG have some vital qualities such as data confidentiality, integrity verification, capacity and robustness, which are crucial factors to achieve successful implementation of steganography process in data security system. The effectiveness and properties of the stego image can be evaluated by some specific measures like mean squared error, root mean squared error, peak signal to noise ratio and structural similarity index matrix to analyse the image quality.

Drawback of this proposed is that: there is low capacity of hidden medium, in our study we will try to solve this kind of problem.

2.8.4 Fourth study

The study of Santosh Kumar Singh, Dr. P.K.Manjhi, Dr. R.K.Tiwari 2019 [16], **Cloud Computing Security Using Steganography,** Paper, Journal of Emerging Technologies and Innovative Research, Volume 6, Issue 6.

With huge benefits cloud computing also brings with it concerns about the security and privacy of information. Now a day's cloud computing is used by smart mobile applications so there are some security and privacy concerns on data provided by the cloud providers.

In this paper, they demonstrate how Steganography, which is a secrecy method to conceal information, can be used to enhance the security and privacy of data maintained on the cloud by mobile applications.

In this model, user will select an image, after that enter the data and the keys as the input now this input will be used by the steganography application, which is installed on the user's mobile device. The steganography application converts the inputs and produce stego image to be accumulated on the cloud. As we know internet connection is must for cloud access. When used want to access the data which is on the cloud, he has to use steganography application and he has to input the key if key matched then user easily and safely access the data.

In this paper proposed steganography application can be used for data security without others involvement. The proposed system will work efficiently with the key, but if he/she loses the key, then the system does not have any provision to recover the key, so in this case a user might cause lose the data. This is the serious drawback on the proposed system. Proposed system is only applicable for limited data so in future they may try large data processing. In the future they can say, cloud and proposed model will work together in efficient manner.

2.8.5 Fifth study

The study of Amel Elamin Elsheikh Elamin 2019 [67], **Secure Data on HTML Web Page using Steganography with Encryption and Compression Technique,** A Thesis Submitted in Partial Fulfillment of the Requirements of Master Degree in Computer Science.

The model was built with three level techniques; **first level** it encrypts the secret message using ElGamal Elliptic Curve Cryptography algorithm so the receiver cannot obtain the message unless by the decryption. **Second level** compress the output from the previous

level result using Huffman Coding by applied Canonical Huffman Coding to reduce the size of compress header. The **last level** uses Steganography techniques to hide the compressed message into one of the HTML webpages contents by adding comments for tags.

Among the drawback of the system is that; it just based on image steganography, which it can't hide any other media inside the image except text file.

We will try to solve the problem encountered by previous model in the way that; we will use very suitable algorithm for hiding and securing transmission of data in cloud computing, more so we need to make our system to acquire huge data for transmission or processing.

Chapter (3):

Methodology

Chapter 3

3.1 Introduction

In this chapter, we present the analysis of the model and its description with some examples of how this model will work. More so, we present the design of the model. Then Implementation.

3.2 Analysis

Secret messages and information's processed or shared via internet are commonly attacks as the internet is considered not completely secured, where discussed in chapter 2 the confidentiality of a messages could be affected by due to different reasons like Excess privileges, lack of security around database, etc., and it can be secure by encryption or hiding secret message in cover image.

3.2.1 Description of current Saas System:

In this section we will analyze current Saas System for hiding secret message in cloud, we will summarize it features, drawback. The study it as follow:

- Prof Dr. P. R Deshmukh, Bhagyashri Rahangdale **"Data hiding using video steganography".**

They proposed the Hash Based Least Significant Bit Technique for Video Steganography

which perform insertion of bits of text file in video in the least significant bit position of RGB pixel as per hash function. In this way it includes Encoding and Decoding process for hiding message and extracting message respectively.

In this technique steganographic tool is developed in MATLAB software which perform Encoding and Decoding. First of all, text will be embedded within the video by using the steganographic tool. This stego video file is again applied to steganographic tool to decode embedded data [64].

3.2.2 Problem of current Saas System:

Among the drawback of current Saas system is as follow:

1. Using one technique for security which is Steganography technique, not make us assure about confidentiality of data.
2. Quality of Cover image used is too large, which can make the system slow during the execution.
3. Low level of security due to non-availability of cryptography technique.

3.2.3 Description of New Saas System:

In this research, we work to solve confidentiality and privacy of data issues in cloud, we will design a system to maintain security of plain text only. And also try to make the level of security to be high by proposing two layers of techniques for secure data while users are sending the secret messages over the internet. In summary, model consist of sender who will send the plain text, and plain text will be encrypt using AES algorithm, then hiding messages inside the video using LSB algorithm; which now becoming stego video after hiding, stego video will now send to Cloud storage for decrypting, then text message.

3.2.4 Model of New secured Saas System:

Proposed model consists of client's side, which is for Embedding secret message and for Extracting the secret message, the below diagram shows how the model works:

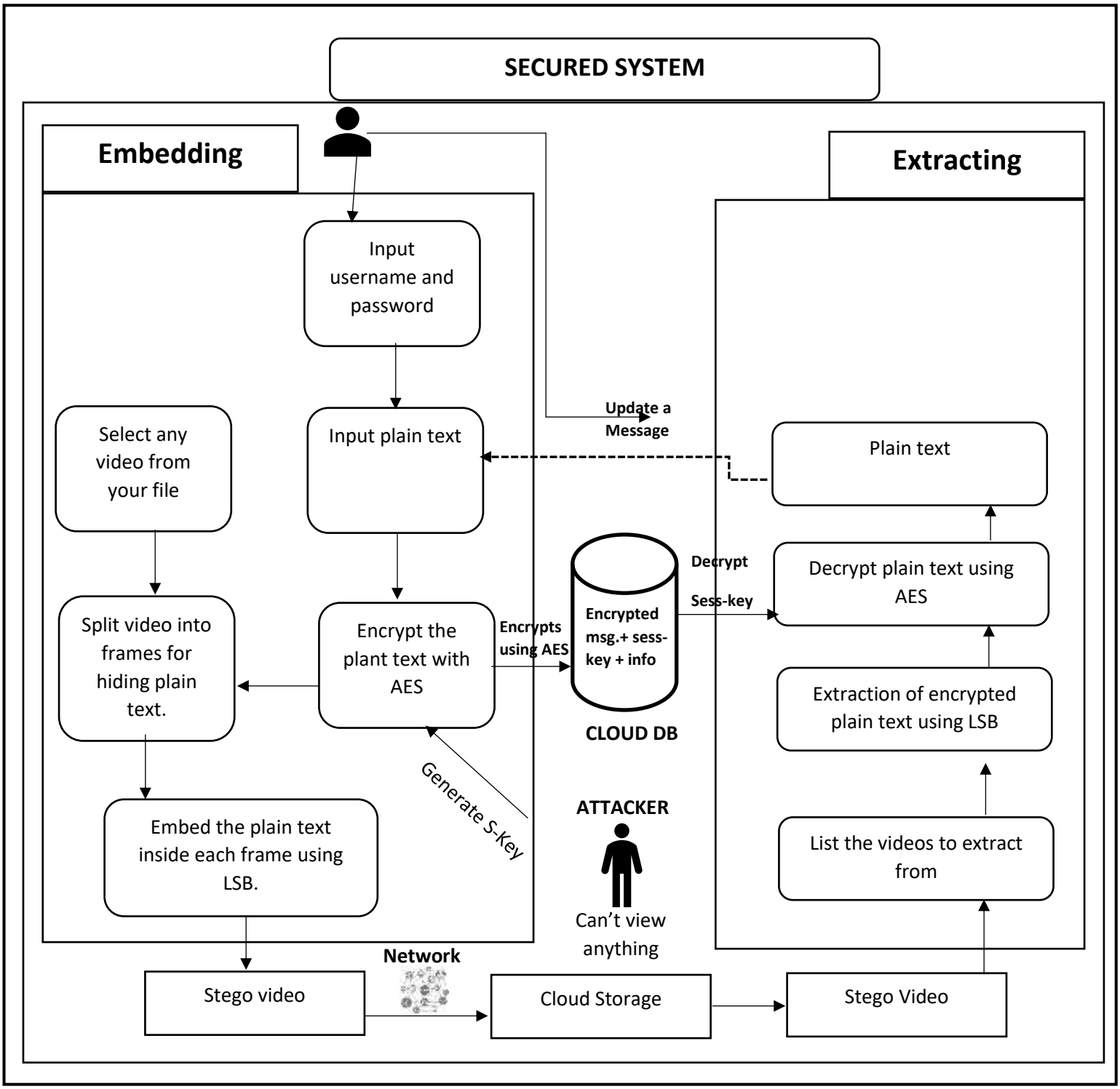


Fig 3.1 – Proposed model.

- **Embedding secret message**

While user want to embed secret message these are the following procedures which he needs to follow:

1. **Input username and password:** User must enter his/her username and password for user authentication and authorization.
2. **Input secret message and select video:** after validation of user account, user will enter his/her secret messages follow by intended video wish to use for hiding secret messages, immediately after this, the system generate session key.
3. **Encrypt the secret message:** after generating the session key, we use AES algorithm for encrypt the secret message and then store into Local database.
4. **Embed secret message:** encrypted message will now embed inside video frames using LSB algorithm which is now became stego video, then, stego video will send over the internet or to cloud storage.
5. **Local database:** is comprises of encrypted message, session key, and secret key which can help the user for retrieve his/her info while need to update his/her messages.
6. **Send to cloud storage:** after finishing of encryption and hidden, system will send the stego-video to cloud storage.

- **Extracting secret messages**

While user want to extract secret message for cloud storage these are the following procedures, he/she needs to follow:

1. **List of Stego-video:** System will list all the stego-video which has been uploaded on cloud storage.
2. **Extracting the secret message:** we use LSB algorithm to split stego-video to frames and to images, and choose specific image which the secret message was hidden.
3. **Checking local database for s-**key and session key: the system check for the user's secret key and session key.
4. **Decrypt secret message:** system decrypt secret message from frame of selected stego-video using AES algorithm and show to the message to user.

5. **Update secret message:** user can update his/her secret message using the same session key and secret key password used at the first upload.

3.2.5 Feasibility study of New Secure System:

In this Session we are going to identify the possibility of improving an existing system, and developing a new system and produce a refined estimate for further development of the system, and the outcome of the study will give us problem scope instead of solving the problem. These are the following feasibility which will carry on during our research:

1. **Technical Feasibility:**

In this research, there are different technical capability and resources to execute the plan on time and within budget, and also our project is web-based application which comprises of the following technical material:

1. Python language with Django.

2. Javascrispt.

3. Google Collaboratory software.

4. Google Drive Storage.

5. Visual Paradigm for UML 64bit_10_0_sp1.

6. The system will work on cloud hosting system which comprises of 12GB of Ram and 127GB of Hard disk.

7. PC of 6GB ram and 1 TRB.

Each technology are freely available and technical skills required are manageable. Time of the product development and the case of implementing using these technologies are synchronized.

Initially the web application will be hosted on local host, then now transfer it on any free cloud hosting for testing and evaluation.

From these it’s now cleared that our project is now technical feasible.

2. Economic Feasibility:

In this section, we will make sure that the study cost and benefit of the project is analyzed. We firstly analyze the cost of our system, which shows in the Table below:

A. COST

Table 3.1: cost of the system:

Items	Consist of	Cost
Technical	1. Pc of 6gb ram and 1 TRB hardisk	$600
	2. windows 10, Sublime, python, Xampp Apache.	$300
Development	1. Planning:	1 month
	2. Implementation: it just a personal work,	2 months.
Operational	1. Cloud hosting	25gb space + 2gb ram Monthly.
	2. Internet service	4Gb or 5Gb network
	3. Technical Support	$300 monthly.

B. Benefit(profit):

As we all know that the benefit of any system maybe tangible or intangible, we classified our own benefit as intangible one, which listed below:

1. Will gain high level of security.
2. Easiness of using.
3. Free service of secured system.
4. Access to the system from any place and any time.

3.2.6 Research Plan and Team:

In this section, we should a Gantt graph to demonstrate the plan and team of our System which will make works processing clear to us, as showing in the Figure below:

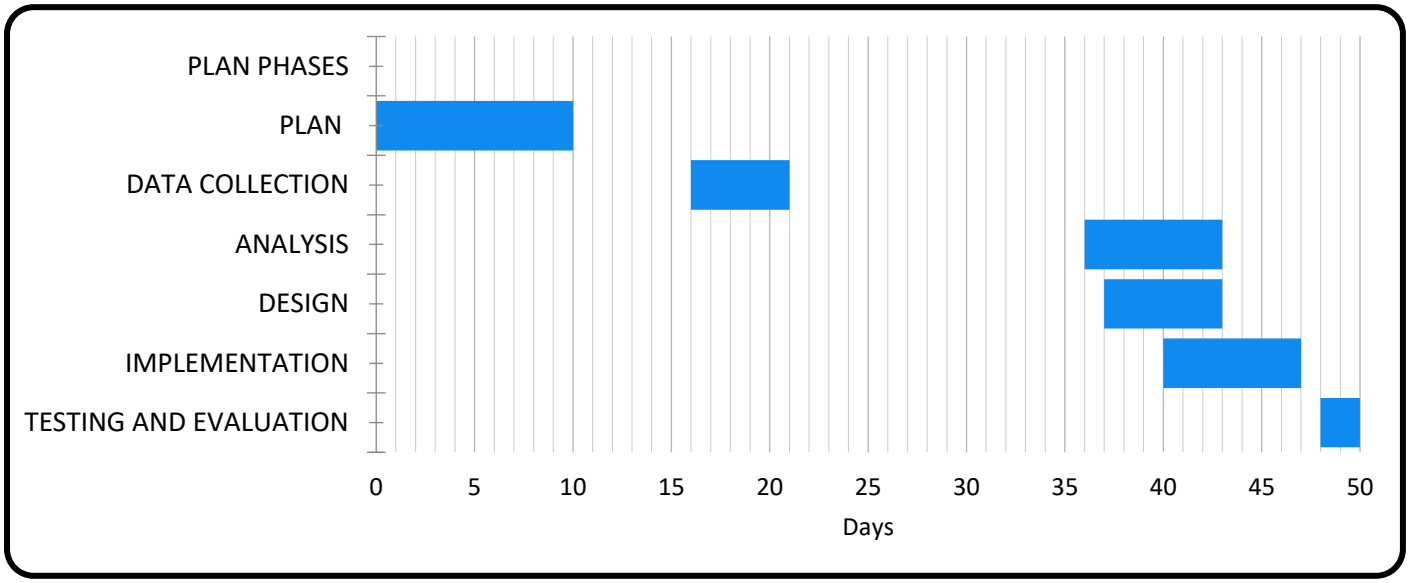


Fig 3.2 – Gantt diagram showing the plan and team of the work.

3.2.7 Process analysis

In the session, we are going to document the current processes, or the needed core processes of a project that are going to be handled with software, which are as follow:

1. **User types**
   In our research, our user types are as follow:

   1. Administrator.
   2. Client.

2. **User types processing**

In this Session we are going to discuss each process which be carry out from User, we need to classify the processing into two different parts:

A. Administration permission:

1. **User privilege**: Administrator is in charge of given each user privilege of access to the proposed system uploaded on the cloud.
2. **Creation of account:** each user must have an account for login process; which consist of email and account.

B. User permission:

1. **Video selection:** user need to select specify video which intent to use for hide secret message.
2. **Input message:** user need to enter his/her secret message which intent to hide on selected video.
3. **Update:** User can update his/her message.

3.2.8 Use case Diagram

In this section, we will present a use diagram which serve as a behavior of our system and help us to capture requirement of the system, and it help us describe the high-level functions and scope of system, and also identify the interactions between the system and actors. The diagram is as follow:

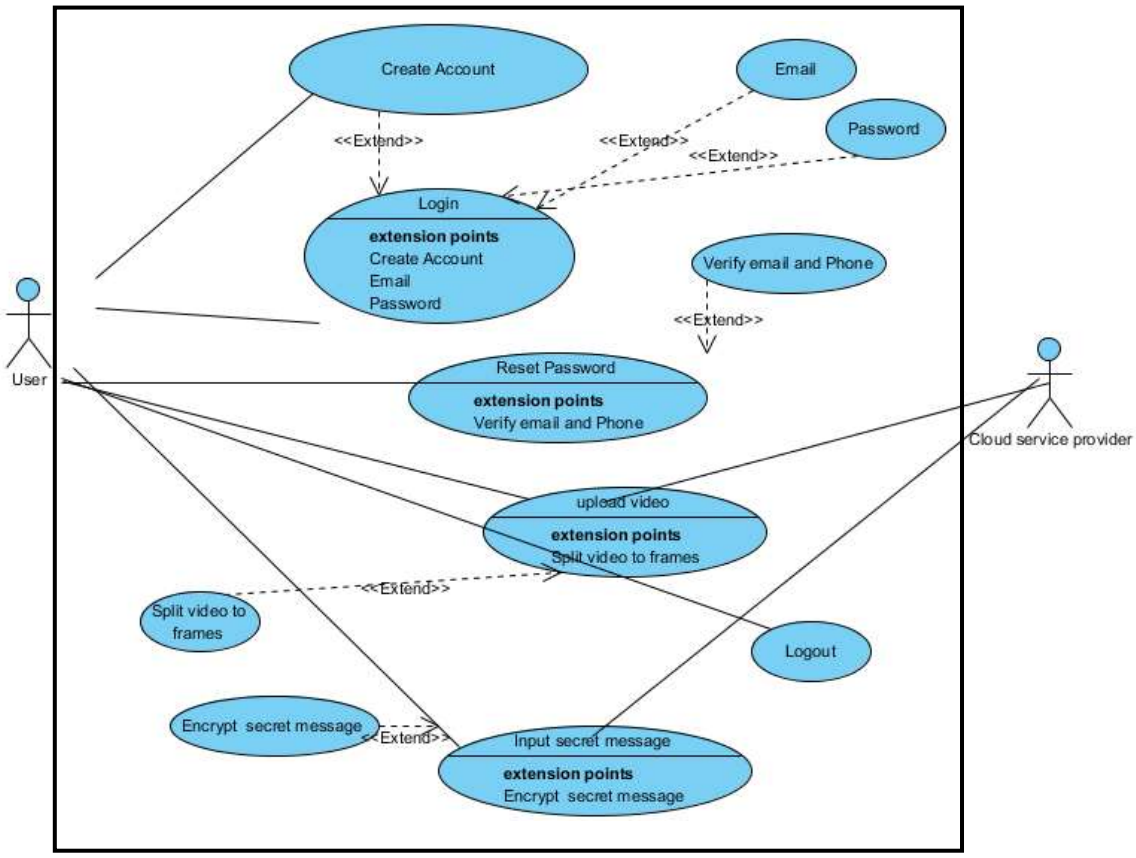


Fig 3.3 – System Use Case Diagram.

3.2.9 Sequence Diagram

In order to achieve the functions of the model, these steps of prototyping methodology are be followed:

Creation of User Account: To create a new user account, the following is done. Step (1) Admin add new user by enter his/her name, password, password confirmation and save into the database.

Step (2) then Admin grant the user permission.

Step (3) Successfully created user Account.

Figure 3.3 below shows the sequence diagram for creation of account.

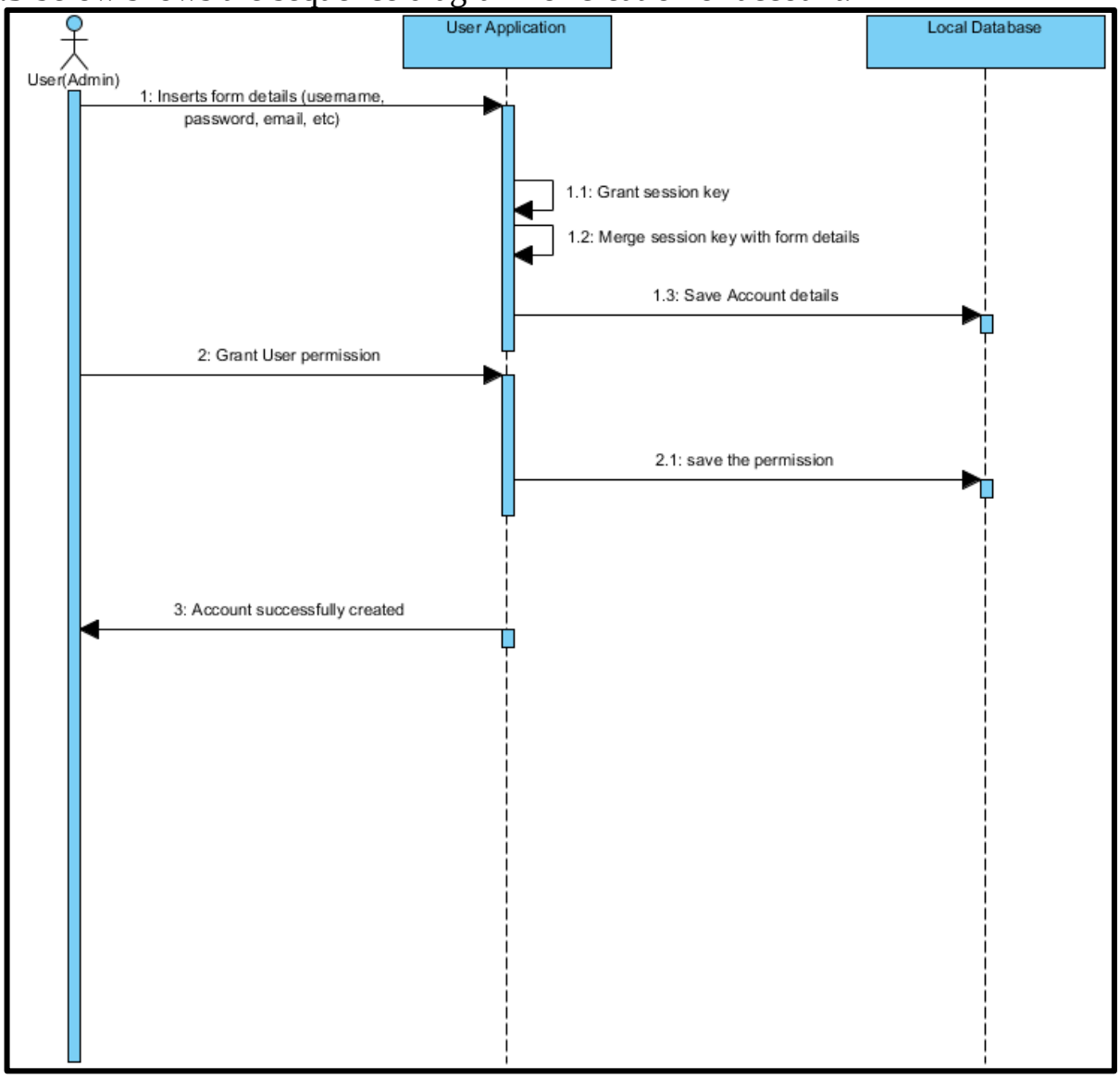


Fig 3.4 – Sequence Diagram of Creation of Account.

User login to Account: For a user to login to his created account

Step (1) the user inserts his username and password in login form

Step (2) the application checks the details from local database for verification.

Step (3) the application merges the entered data (username and password) and generates session key.

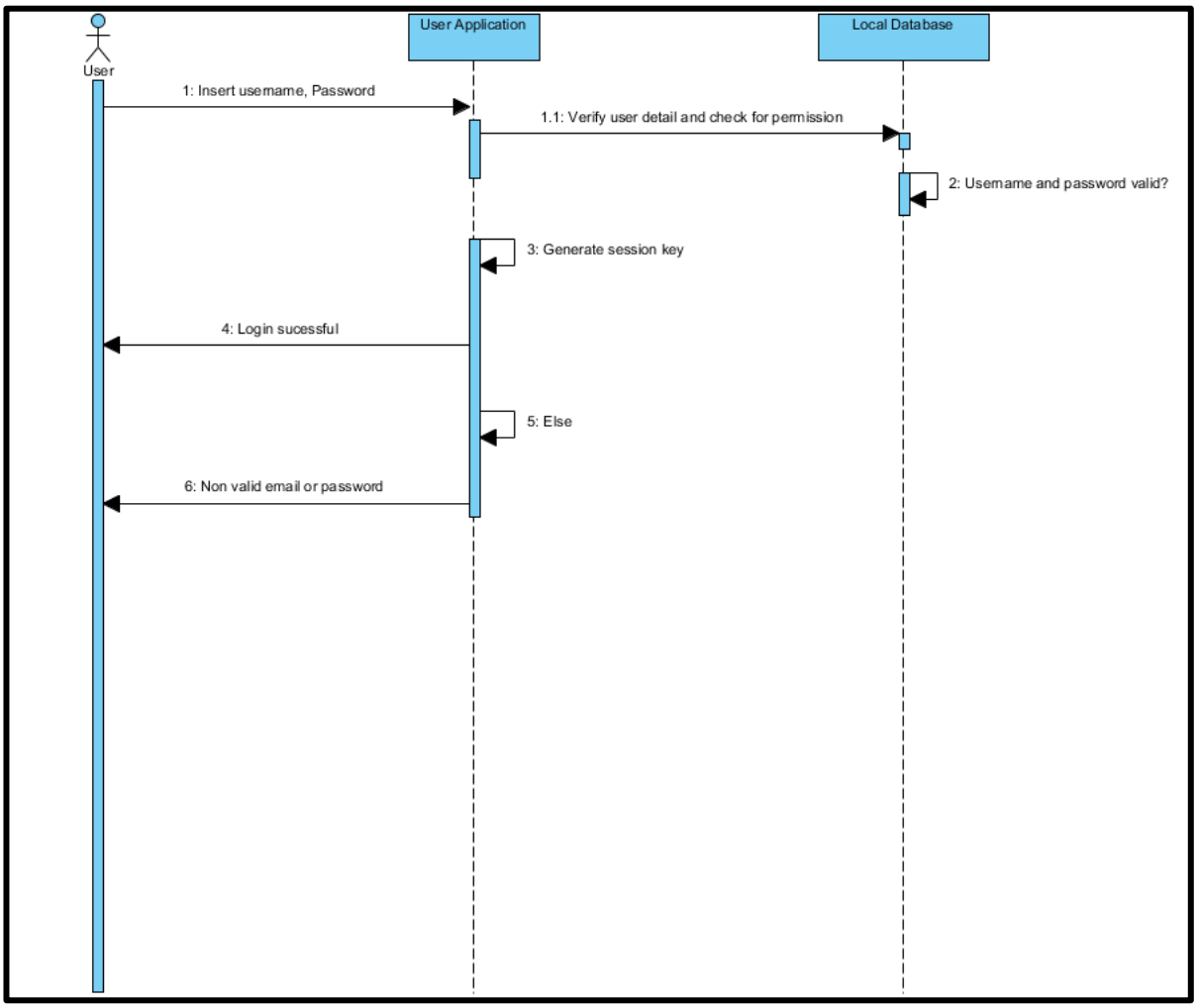


Fig 3.5 – Sequence Diagram of User login to Account.

Embedding Secret message: For a user to embed and encrypt secret message inside selected video, the following steps will follow:

- **User Login:** user will login with his/her valid account details, by enter his/her Username and Password, system will generate session key for the user.
- **Video Selection and message entering:** after successfully login of the User, User need to select a video which intended to hide a message into, and encrypt entire message before hiding inside the video, we encrypt message using AES (Advanced Encryption Standard) algorithm; is a symmetric block cipher, which also known as secret key, chippers use the same key for encrypting and decrypting, so the sender and receiver must both know –and use – the same secret key. we will hide encrypted message into the video by splitting the video into frames, then frames to image by using LSB (Least Significant Bit) technique in which we hide encrypted messages inside an image by replacing Least significant bit of image with the bits of encrypted message to be hidden. After hidden encrypted messages into image, all the images will merge together to form stego-video, then application will generate secret key and upload stego video directly to the cloud Storage.

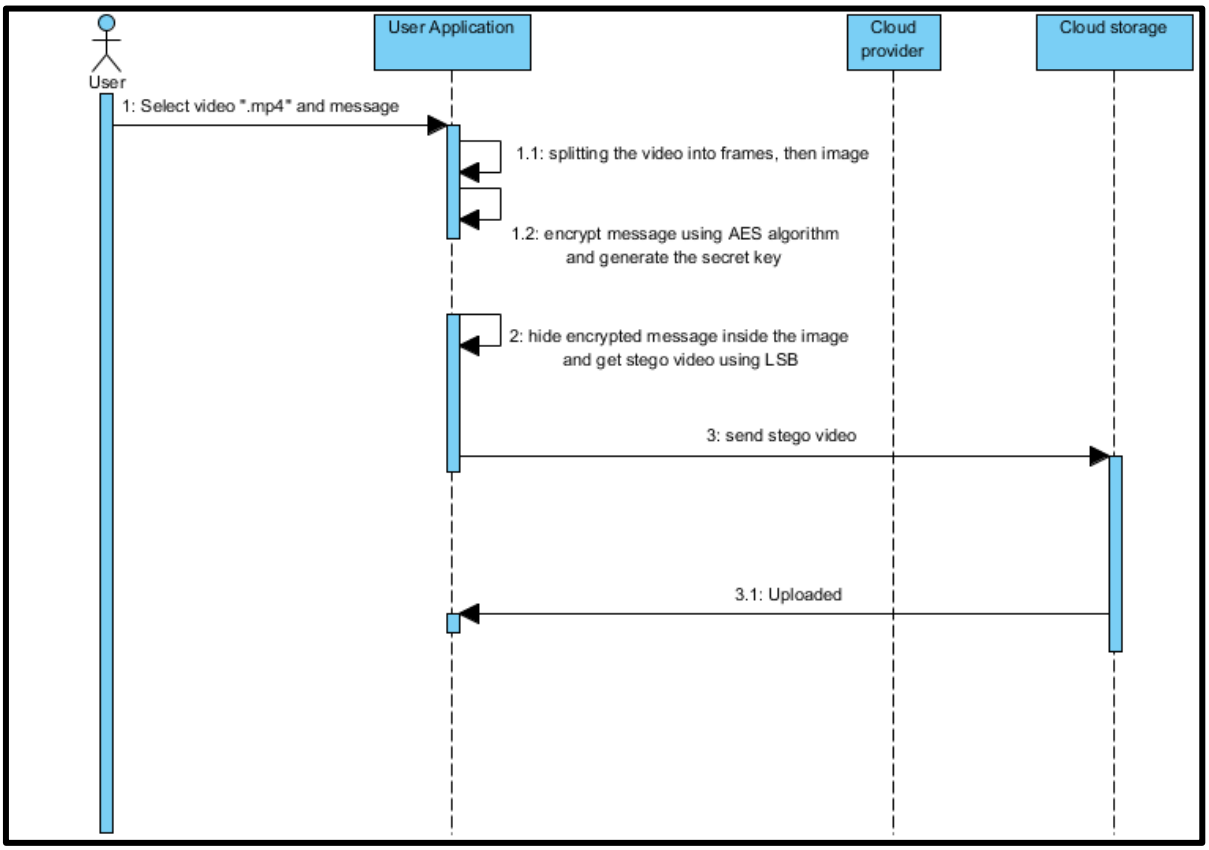


Fig 3.6 – Sequence Diagram for Embedding secret message.

Extracting Secret message: after the embedding process is completed, the sender sends the stego video into the cloud storage. We need to split the video again in order to extract the secret messages, these are the following step to extract the secret message:

- **List of Stego video:** after successful login of user, Application will list all the stego video which has been uploaded on cloud Storage, user select a video he/she want to decode a secret message from, Application kindly request for secret key generated with AES algorithm, then application split the video again using LSB technique for extracting secret message, then display plain text message.

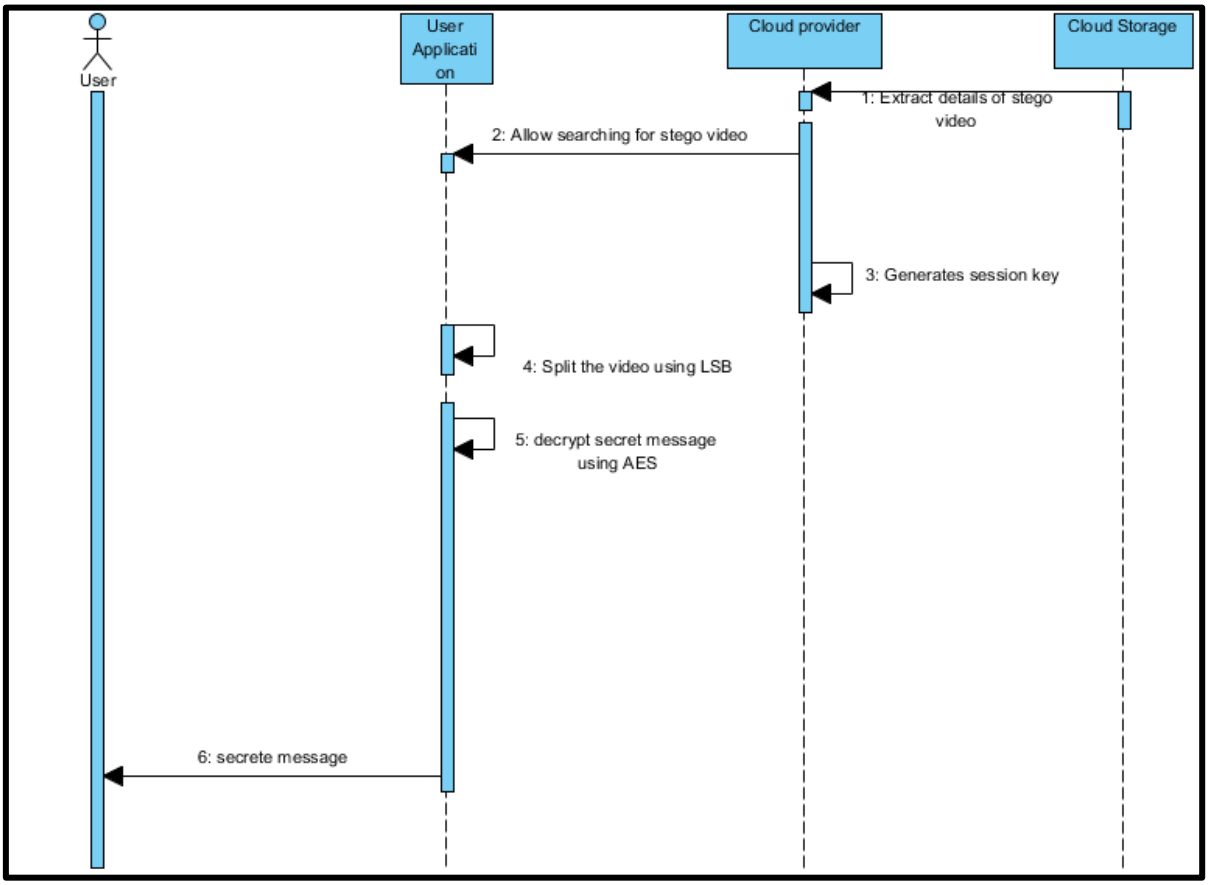


Fig 3.7 – Sequence Diagram for Extracting secret message.

3.2.10 Design

In this section, we present the design of the proposed model and how the underlying system will look, designing the database, process design and interface design:

1. **Database Design**

Database design is the organization of data according to a database model; we determine what data must be stored and how the data elements interrelate with each other. To implement the proposed model different database types could be used either it is relational or object oriented, we use a relational database MySQL to implement the proposed model. MySQL is an open-source relational database management system.

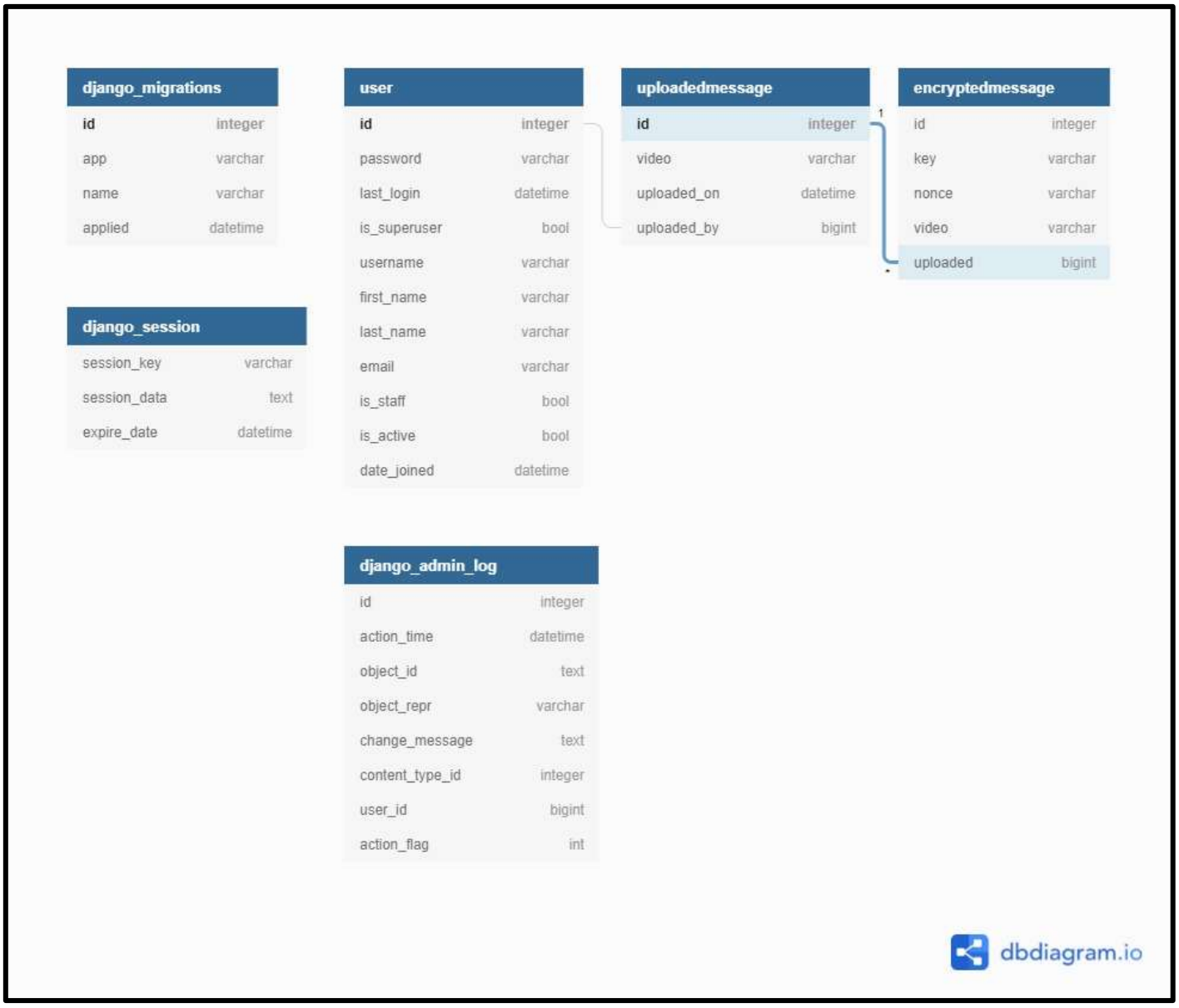


Fig 3.8 – Database Design.

2. Data Dictionary

The following tables represent data dictionary for our model, which as follows:

auth_group

Column	Type	Null	Default	Links to	Comments	Media (MIME) type
id *(Primary)*	int(11)	No				
name	varchar(150)	No				

auth_group_permissions

Column	Type	Null	Default	Links to	Comments	Media (MIME) type
id *(Primary)*	bigint(20)	No				
group_id	int(11)	No	auth_group -> id			
permission_id	int(11)	No	auth_permission -> id			

auth_permission

Column	Type	Null	Default	Links to	Comments	Media (MIME) type
id *(Primary)*	int(11)	No				
name	varchar(255)	No				
content_type_id	int(11)	No	django_content_type -> id			
codename	varchar(100)					

core_encryptedmessage

Column	Type	Null	Default	Links to	Comments	Media (MIME) type
id *(Primary)*	bigint(20)	No				
key	varchar(200)	No				
nonce	varchar(200)	No				
video	varchar(100)	No				
uploaded_id	bigint(20)	No	core_uploadedmessage -> id			

core_uploadedmessag

Column	Type	Null	Default	Links to	Comments	Media (MIME) type
id *(Primary)*	bigint(20)	No				
video	varchar(100)	No				
uploaded_on	datetime(6)	No				
uploaded_by_id	bigint(20)	No	core_user -> id			

core_user

Column	Type	Null	Default	Links to	Comments	Media (MIME) type
id *(Primary)*	bigint(20)	No				
password	varchar(128)	No				
last_login	datetime(6)	Yes	*NULL*			
is_superuser	tinyint(1)	No				
username	varchar(150)	No				
first_name	varchar(150)	No				
last_name	varchar(150)	No				
email	varchar(254)	No				
is_staff	tinyint(1)	No				
is_active	tinyint(1)	No				
date_joined	datetime(6)	No				

core_user_groups

Column	Type	Null	Default	Links to	Comments	Media (MIME) type
id *(Primary)*	bigint(20)	No				
user_id	bigint(20)	No	core_user -> id			
group_id	int(11)	No	auth_group -> id			

core_user_user_permissions

Column	Type	Null	Default	Links to	Comments	Media (MIME) type
id *(Primary)*	bigint(20)	No				
user_id	bigint(20)	No	core_user -> id			
permission_id	int(11)	No	auth_permission -> id			

django_admin_log

Column	Type	Null	Default	Links to	Comments	Media (MIME) type
id *(Primary)*	int(11)	No				
action_time	datetime(6)	No				
object_id	longtext	Yes	*NULL*			
object_repr	varchar(200)	No				
action_flag	smallint(5)	No				
change_message	longtext	No				
content_type_id	int(11)	Yes	*NULL*	django_content_type -> id		
user_id	bigint(20)	No	core_user -> id			

django_content_type

Column	Type	Null	Default	Links to	Comments	Media (MIME) type
id *(Primary)*	int(11)	No				
app_label	varchar(100)	No				
model	varchar(100)	No				

django_migrations

Column	Type	Null	Default	Links to	Comments	Media (MIME) type
id *(Primary)*	bigint(20)	No				
app	varchar(255)	No				
name	varchar(255)	No				
applied	datetime(6)	No				

django_session

Column	Type	Null	Default	Links to	Comments	Media (MIME) type
session_key *(Primary)*	varchar(40)	No				
session_data	longtext	No				
expire_date	datetime(6)					

3. Interface Design

Create account: Admin creates account for the users by filling his details and grant him/her permission to the System. Figure **3.9** shows the design of account creation page.

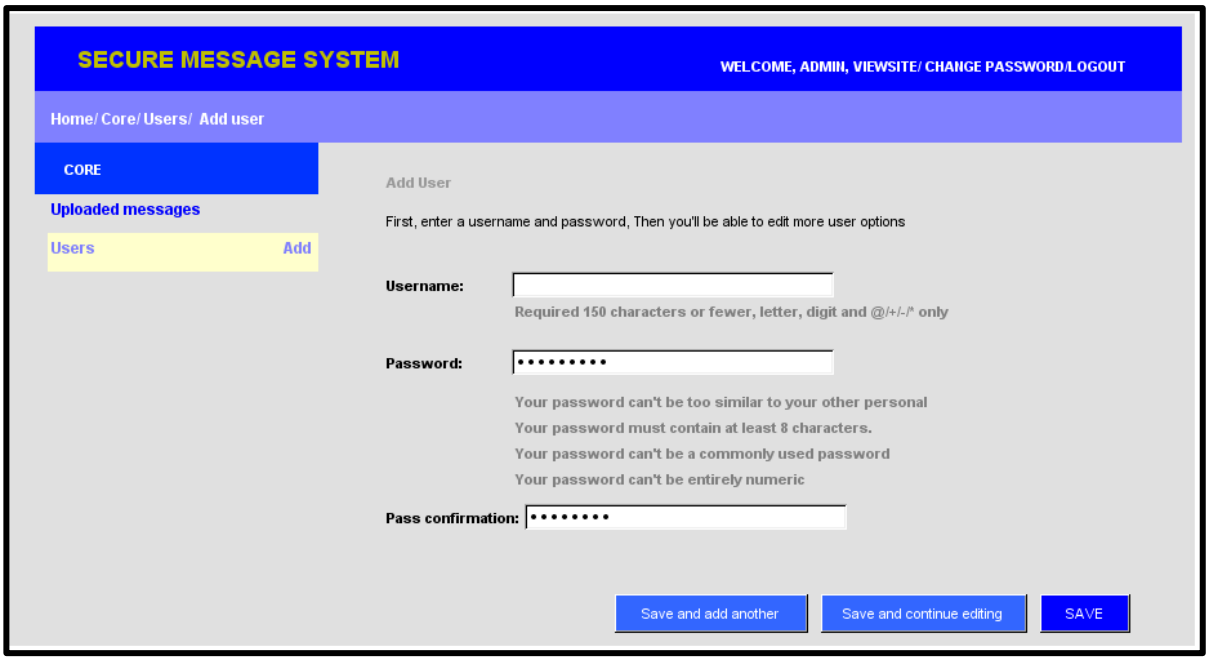


Fig 3.9 – create account interface.

Login to Account: This page allows users to log in to account. **Figure3.10** shows the Design of login to account page.

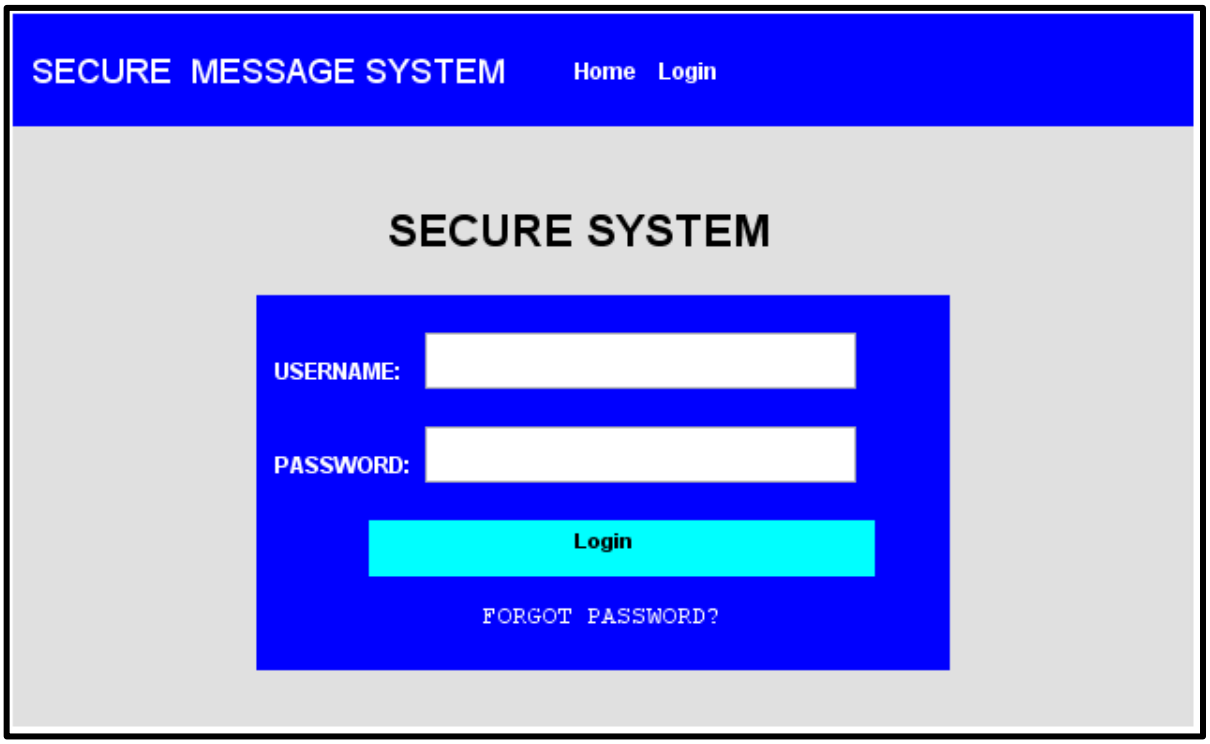


Fig 3.10 – Login-Page Interface.

Home Page: The user can access the home page after entering his correct details. The **figure 3.11** below shows the homepage of the system.

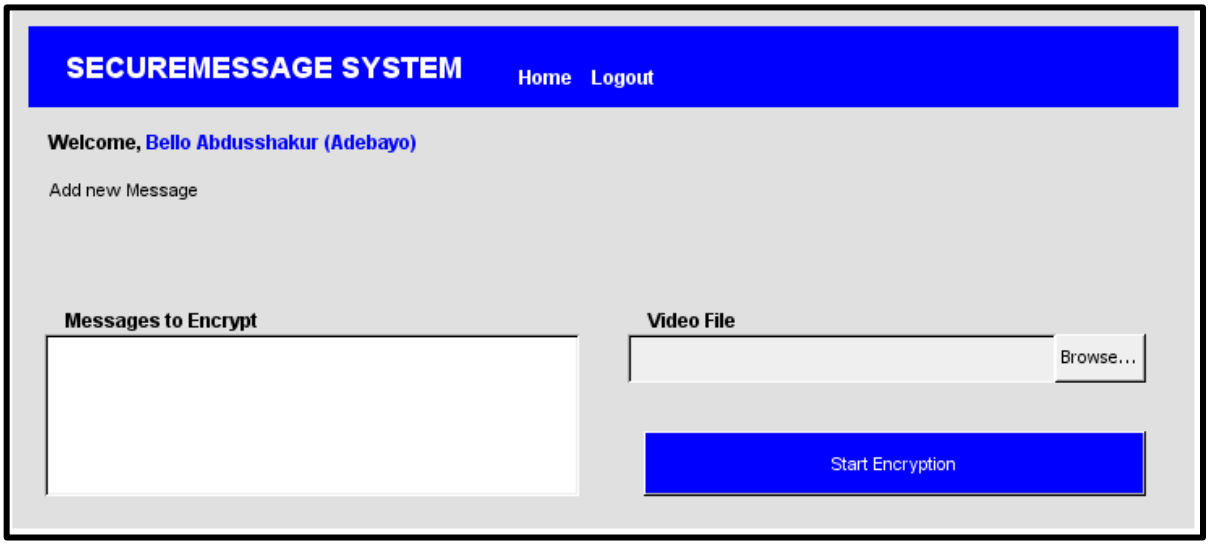


Fig 3.11 – HomePage Interface.

Admin Page: The admin can view the uploaded messages of the users and create the account for the user. The **figure 3.12** below shows the homepage of the system.

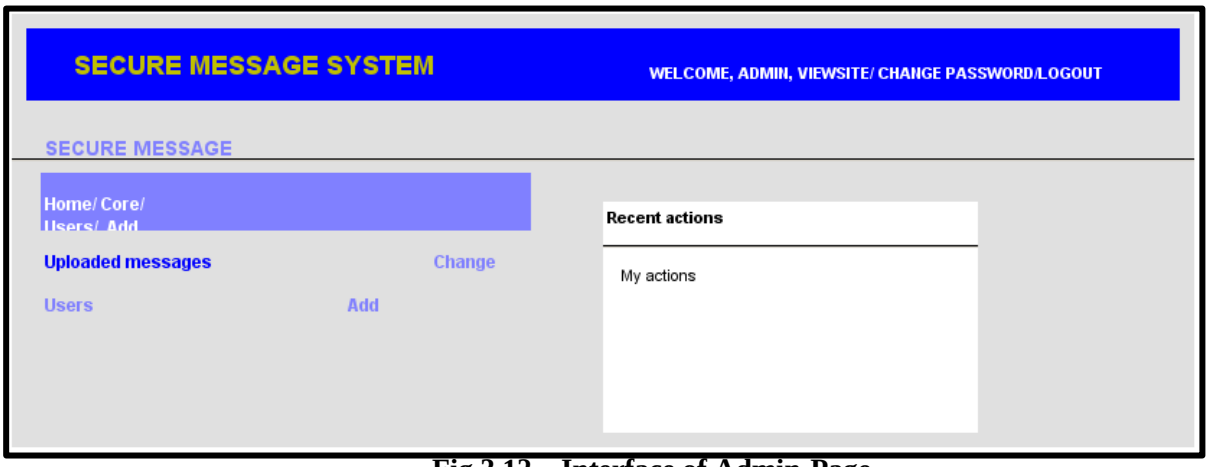


Fig 3.12 – Interface of Admin-Page.

3.2.11 Implementation

In this section, the implementation of our model is discussed and the system, which we built, is described, with introducing used programming language used to implement main parts of the model.

As our proposed system is web based, to implement this we can use several programming languages like Python, PHP, and Java Script. To implement our model python Django is used as a programming language because it is free and widely used and this is just a prototype implementation so we can develop it in the future using other cloud friendly programming languages. Django is a high-level Python web framework that encourages rapid development and clean, pragmatic design. Built by experienced developers, it takes care of much of the hassle of web development, so you can focus on writing your app without needing to reinvent the wheel. It's free and open source and can be embedded into HTML. So, it is used in this work. [65]. The implemented model will be deployed on an open-source and commercial cloud platform (Digital Ocean) with AWS storage. The table below shows the languages and tools, which were used for implementing the model.

Table 3.2: The languages and tools used to implement proposed model

1.	Server-Side Language	Python Djagon
2.	Client-Side Language	Javascript, HTML, CSS
3.	Operating System	Windows 10.
4.	Deployment	Digital Ocean with AWS storage.

5.	Hardware Specification	Intel(R) Pentium(R) CPU 3825U @ 1.90GHz 1.90 GHz, RAM: 6GB.

As the prototype website was built with several components figure 3.12 show the homepage of the system

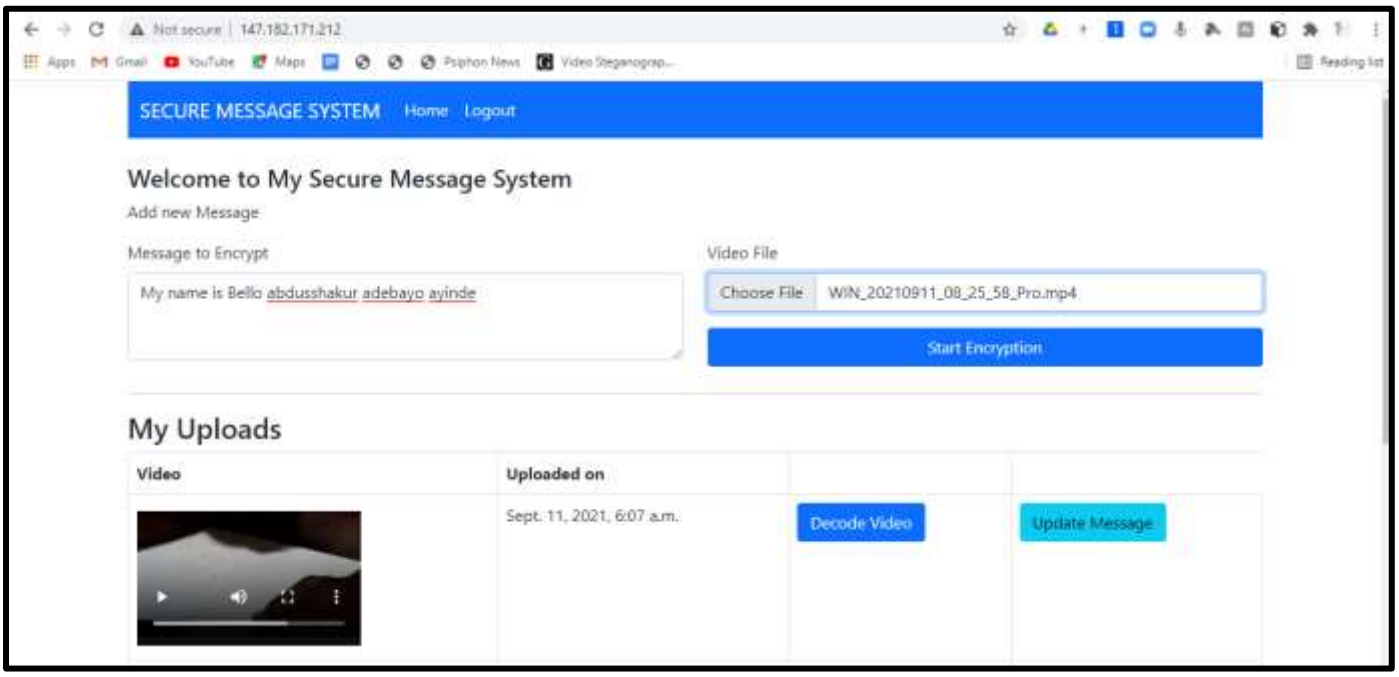


Fig 3.13 – Homepage of the System.

Summary

In this chapter, we presented analysis of some model uses to prevent man-in the cloud attacks, we also built our model to prevent our messages from man-in the middle attacks with its architecture and descriptions. The proposed model is further described using the sequence diagram to model. In addition, we presented the design structure for expected implementation, finally in implementation section, the model was coded (programming) and uploaded to a public cloud environment, the implementation was carried using several tools and software which involves the Python Django language, JavaScript, HTML etc. We presented the main functions of the model which includes (Creation of account, login to account, Embed the message, extract the message and update the message) and the implemented model is deployed on the public cloud.

Chapter (4):

Experiment and Evaluation

Chapter 4

4.1 Introduction

In this chapter, our experiments are presented also with the evaluation of the proposed system to prevent man in the cloud attacks by using AES algorithm which is cryptography techniques and using LSB for video steganography. We used AES algorithm to generate secret key after the user had encrypted message inside the video, while using LSB for hidden secret message inside images of selected videos. We implemented parts of the user authentication and integrity checking process. An analytical study is applied in this work to test the system.

4.2 Experiment

Four experiments are performed on our implementation to demonstrate its ability to check confidentiality of data sent to the cloud and to allow user only authenticated users to access the messages, these experiments can be listed as:

1. Using a wrong password while trying to access user account.
2. Using man in middle attack to see if user messages can be edited while it is being sent or received from the cloud.
3. Using different video sizes to test capacity of the system.
4. Test all model modules.

4.2.1 Experimental Environment and tools

Our experiments are conducted with a laptop (HP250), running Windows 10 (x64 bits) operating system with Pentium (R), with 4 GB memory RAM

4.2.2 Setup a Public Clouds:

We built a website that enables users to send and update a message over the cloud. This website is hosted on Digitalocean online Cloud Platform as a Service as shown in **Figure 4.1, 4.2, 4.3**. The public cloud host. The site can be access using IP address: **147.182.171.212.**

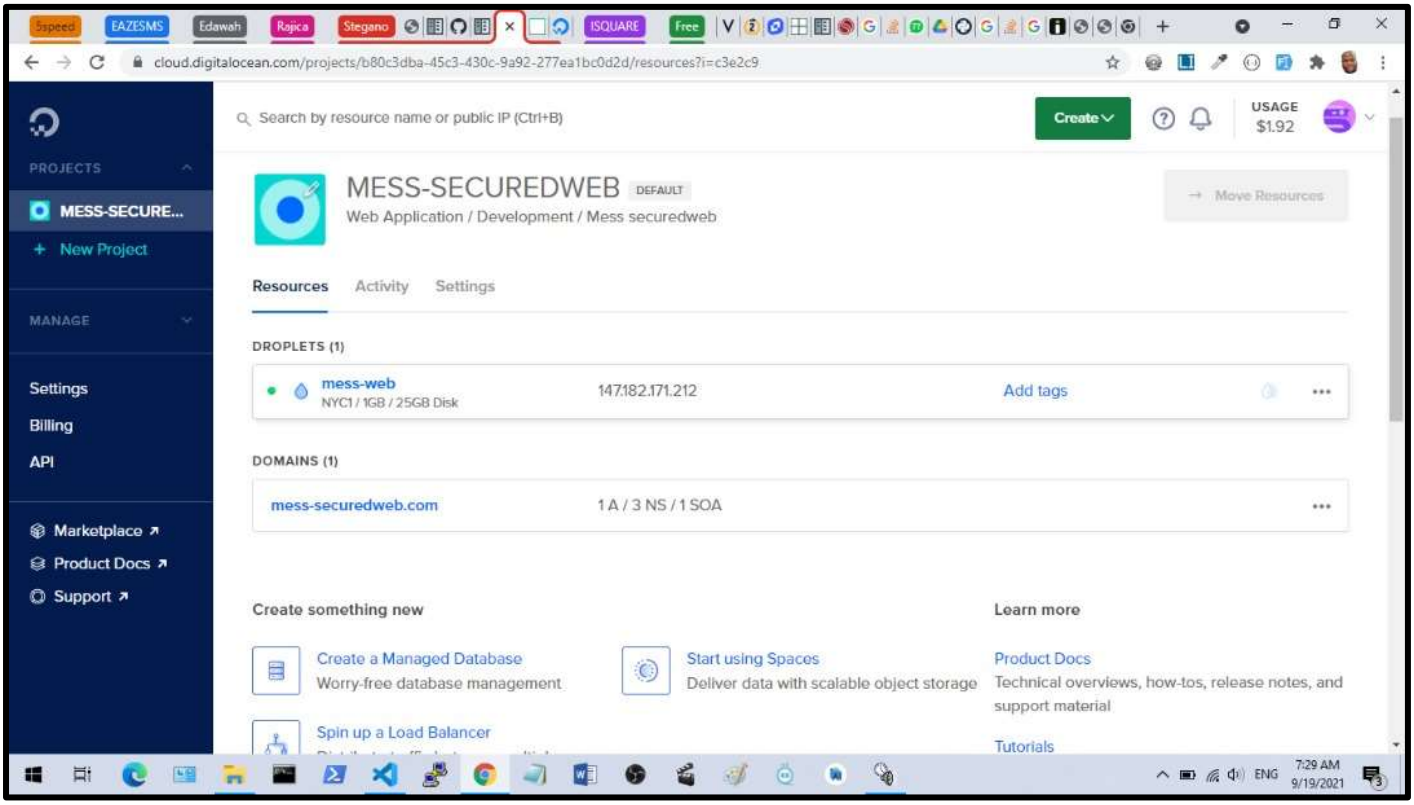


Fig 4.1 – Setup a Public Cloud.

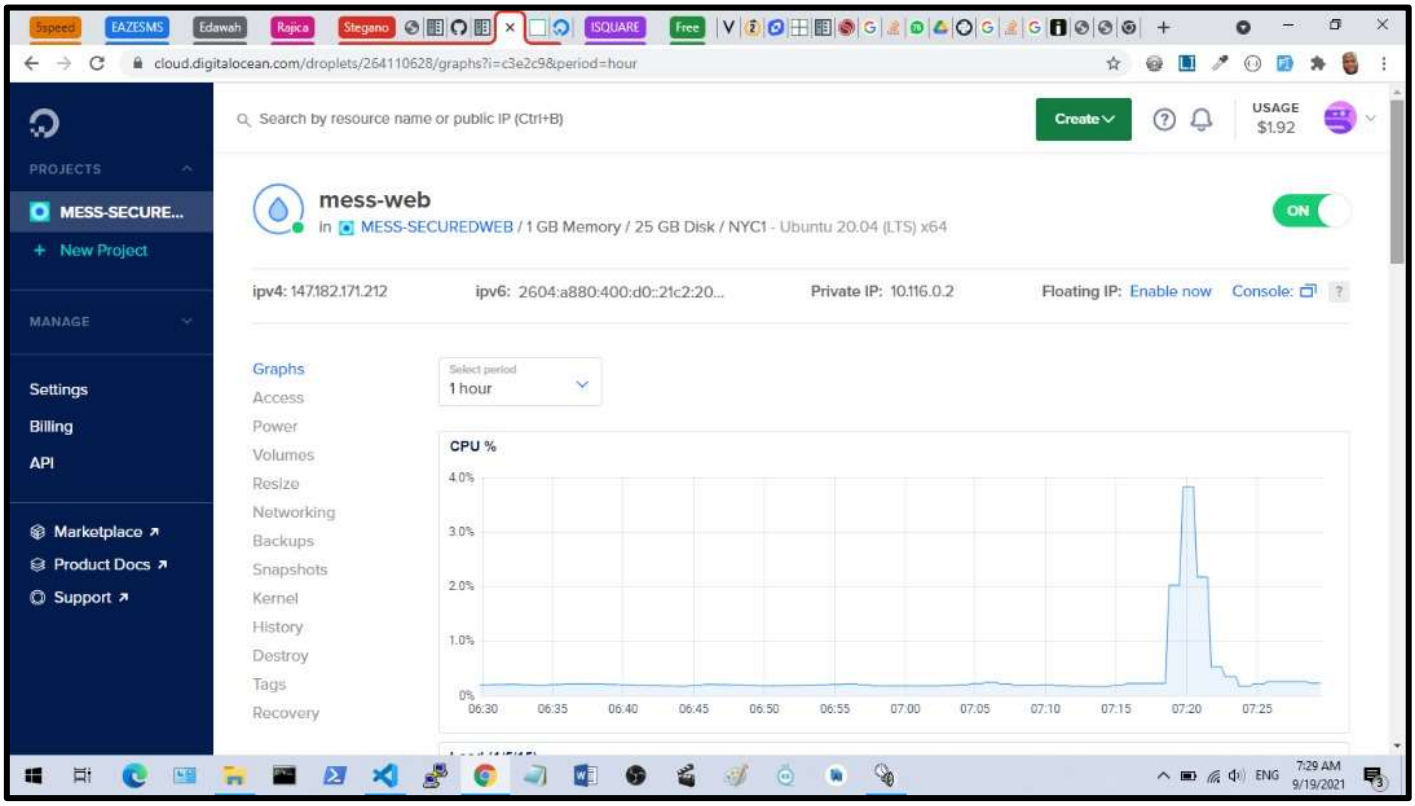


Fig 4. 2 – Showing the speed of CPU server.

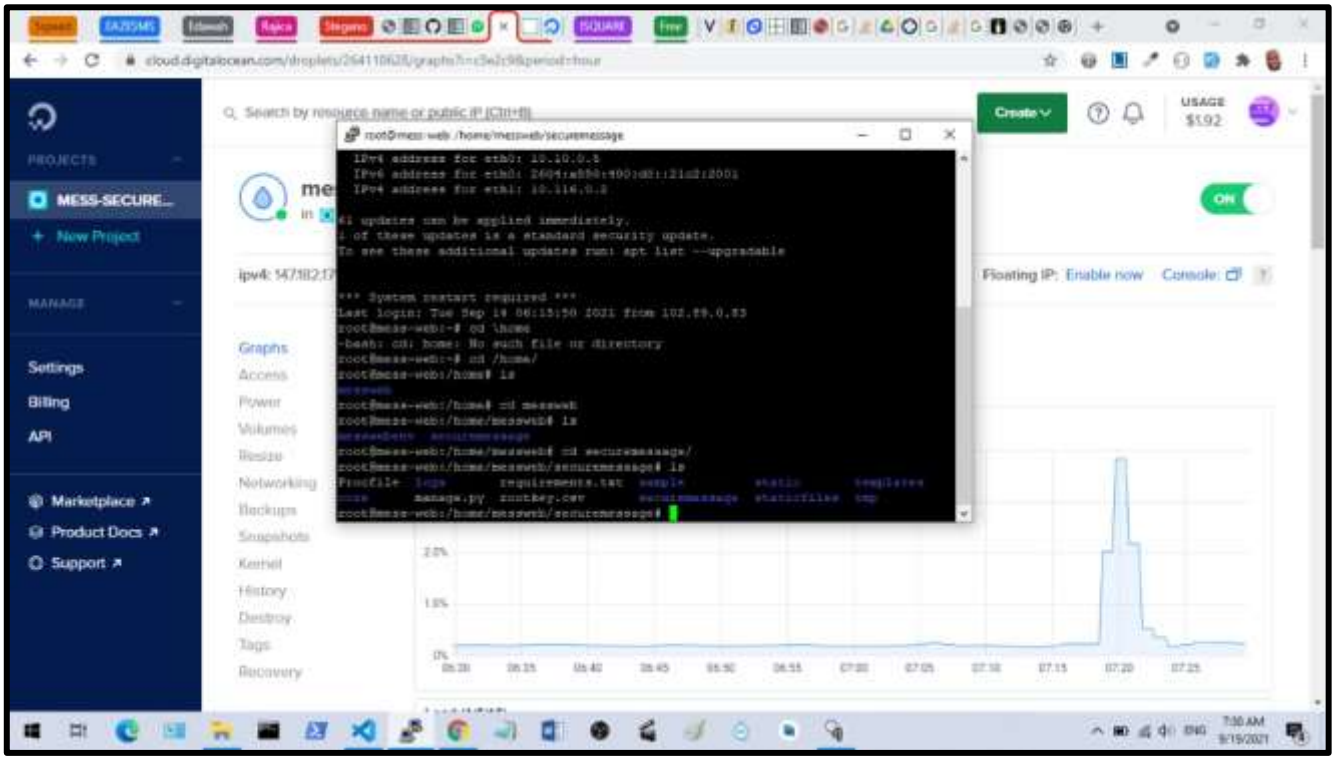


Fig 4. 3 – Running the System on the Virtual Environment.

4.2.3 Model Experiment:

After we got ready of different videos and messages to send, four different types of experiments have been constructed.

1. **Experiment 1, Accessing the User Accounts Using a username/ password to access account:**

The first experiment is to use a wrong username/ password. The model proved that account cannot be accessed using wrong password as seen in **figure 4.4**.

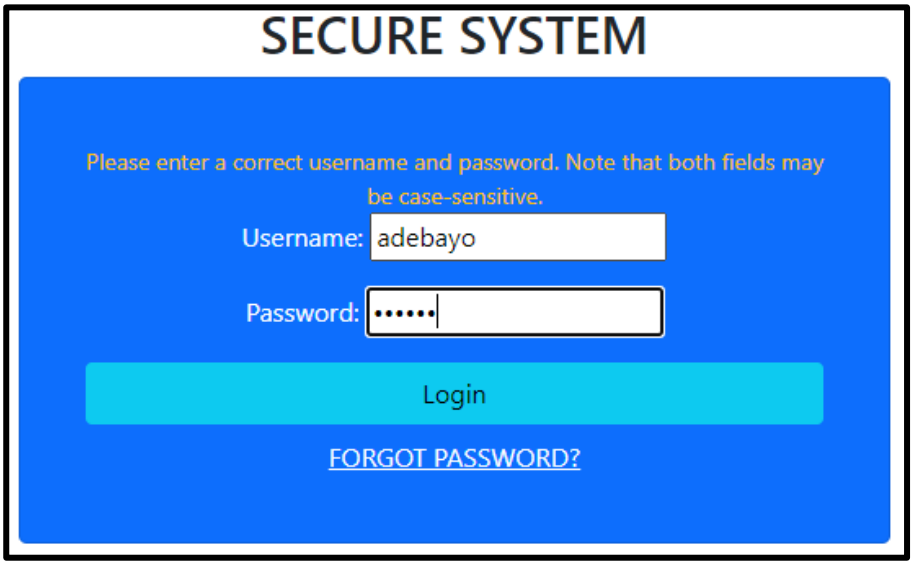


Fig 4.4 – Experiment One.

2. Experiment 2, Sending the secret message over a network to the cloud:

while sending a secret message over the internet to the cloud and a hacker manages to gets illegal access to the message; can he copy or edit the message in the middle. As files are encrypted and hided inside the video while encoding and decoding even if the hacker gets access to the stego-video it would be difficult to decrypt them as he cannot get the private key of the user or cloud provider. Fig 4.5: showing the successful received message.

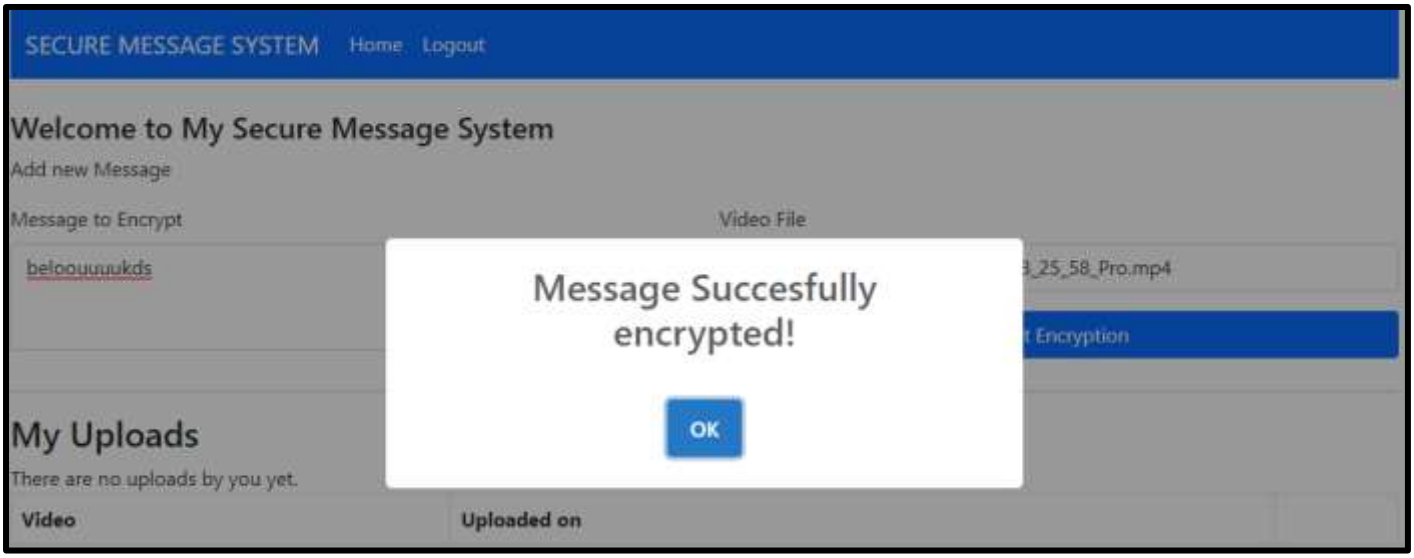


Fig 4.5: Sending the secret over the internet to the cloud.

3. Experiment 3, Update a message many times in the same video respectively:

To test if the system will change the s-key anytime user want to update his/her message, we keep s-key remains once anytime user want to update his message with the same video.

Fig 4.6: Message inside the stego video before update Using the same S-key.

Fig 4.7: Message inside the stego video after update Using the same S-key.

4. **Experiment 4, Accessing to secret message using wrong s-key with invalid session key:**

While user want to decode his/her secret message from stego-video, if the secret key or session key is invalid, the system will display what on the **figure 4.8.**

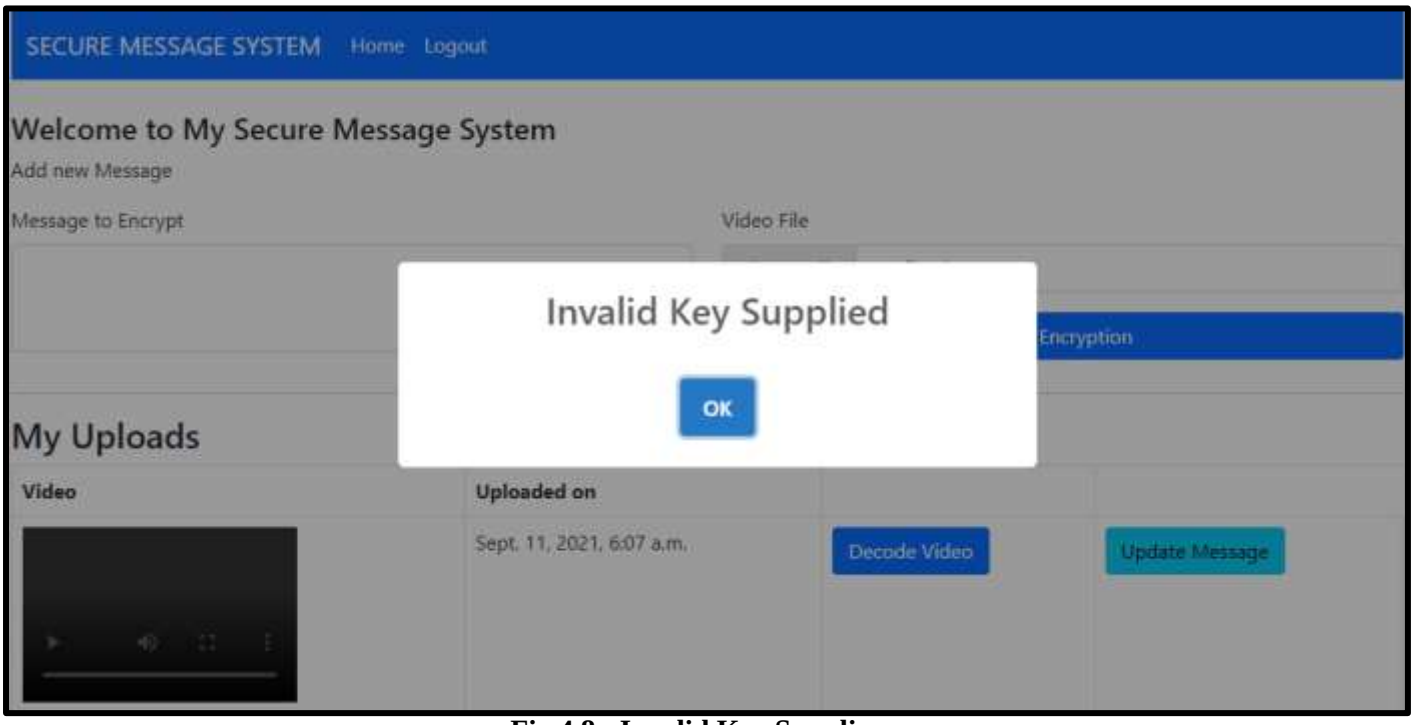


Fig 4.8: Invalid Key Supplies.

4.3 Evaluation

The most important measure in our model is accuracy, in terms of security; it is measured by enabling users to encode and decode his messages securely while transferring to the cloud storage. The other measure is to evaluate the authentication system by trying to access user accounts using wrong login detail (username and password), and also, we evaluate the noisy of the video used to hide message.

4.3.1Accuracy Evaluation:

Our focus is to securely encode and decode secrete message from stego-video while transferring to the cloud. Three experiments were conducted, in order to evaluate the accuracy:

1. While transmitting stego-video to cloud, we make stego-video is not splitted.
2. We ensure the secret-key saved in database in hash format.

Chapter (5):

Results, Conclusion, Recommendation.

Chapter 5

5.1 Introduction

In this chapter, we will conclude our work, results, results discussions, conclusion and recommendations for future studies.

5.2 Results

In this research, we proposed a model using cryptography and steganography techniques which can be used for data security without others involvement, The proposed system will work efficiently with the key, we got the following results:

1. Improved public cloud security for the cloud users by adopting the symmetric encryption system.
2. Also improved public cloud security for the cloud users by adopting the hiding technique using video steganography as cover medium while sending secret message to the cloud.
3. We proposed a new model to secure the user data; the model provides user authentication and confidentiality.
4. The conducted experiments proved that our proposed model is applicable and strong against any attacks from man in the middle.
5. The model protects data while in transmission to the cloud storage.
6. The conducted experiments proves that the model can be used for any video type and size easily and fastly.

5.3 Result Discussion

The model improves the public cloud security by adopting the use of symmetric encryption and LSB technique, in symmetric encryption we use the AES (Advanced encryption system) where a secret key is generated to encrypt a message to create a secure transmission and we use the LSB to hide encrypted message inside the video while sending to cloud storage.

We proposed a new model to secure the secret message against man in the middle attacks; the model provides user authentication and confidentiality; the user authentication is

enhanced by hash function and cryptography and video steganography for confidentiality of data.

Experiments were conducted on the proposed model using with different Video types and sizes, to ensure the ability of the model to allow only authenticated users and ensure the confidentiality of message. The experiments also proves that even the cloud providers cannot modify access the protected files belonging to the users, so the files are protected against cloud breaches even though there is good level of trust between the cloud provider and cloud users. The model also shows that the performance is very effective as less computation power is used to achieve high security.

With this, we have achieved all our research objectives; as we achieved objective (1) in chapter two where we discussed and studied the start of art of security in cloud computing and how man in the middle attacks works. We achieved objective (2) also in chapter (3) where we studied and summarized well-known techniques used to prevent man in the cloud attacks and are being used in cloud computing. We achieved objective (3) also in chapter (4) where we implement and evaluate our proposed model. Finally, objective (4) was achieved as our proposed model was implemented and deployed in a public cloud environment and its accuracy was tested, after several experiments and testing was carried in live public cloud environment, we validated that the model is at an acceptable level and is highly efficient for preventing man in the attacks and ensure the confidentiality of data.

5.4 Conclusion

In this Thesis, we addressed the problem of man in the middle attacks in which he is working against the file sending in public cloud, as so far, we used two level techniques to solve the problem out, which is cryptography and steganography techniques as there is an increasing trend of outsourcing data to remote cloud servers and it is vital to ensure that data are kept properly. We studied the current state of art of security in cloud computing and we analyzed previously proposed models used for preventing man in the cloud attacks. We proceed to developing our model that has two phases; which is embedding and extracting side, embedding comprises encryption and hiding of message before sending to the cloud, while extracting comprises of decryption and extracting of message after it has reached the cloud storage. The model was implemented using various state of art tools and programming

languages and the prototype website was deployed in the public cloud environment. Several experiments were carried and they proved that the model supports strong user authentication, and confidentiality of messages and non-repudiation.

5.4 Recommendation

As future challenges may appear, we recommend the following:

1. They can utilize a key, which represents a set of arbitrary values for selecting frames and embedded image or audio file within a video.
2. They can implement hash function to test integrity of stego-video uploaded on the cloud storage.
3. Using biometric authentication will make the system strong and reliable,
4. Randomly selecting the pixels can utilize for embedding rather than serial selection in the traditional LSB to increase the security and to prevent the hackers from discovering the pixels that have the secret data.
5. Using Asymmetric encryption can make the system fast.
6. Developing a System to be use between more users to communicate with each other.

Reference

1. Ling Qian, Zhiguo Luo, Yujian Du, and Letiao Guo, Cloud Computing: An Overview, ResearchGate, Conference Paper, January 2009.
2. Swati I. Bairagi, Ankur O. Bang, Cloud Computing: History, Architecture, Security Issues, (IJARCE) International Journal of Advent Research in Computer and Electronics (E-ISSN: 2348-5523) Special Issue National Conference "CONVERGENCE 2015", 28 March 2015.
3. Sam Goundar, Understanding Cloud Computing: Victoria University of Wellington, March 2018.
4. Aaqib Rashid, Amit Chaturvedi, Virtualization and its role in Cloud Environment, (JCSE) International Journal of Computer Sciences and Engineering, E-ISSN: 2347-2693, vol-7, Issue-4, April 2019.
5. Raja Mohammed Jabir, Salam Ismail Rasheed Khanji, Liza Abdallah Ahmad, Omar Alfandi, Huwida Said, Analysis of Cloud Computing Attacks and Countermeasures: College of Technological Innovations, Zayed University, 144534, UAE 2019.
6. Aditya K. Sood, Ph.d., Rehan Jalil, Cloudifying Threats Understanding Cloud App Attacks and Defenses: ISACA JOURNAL VOL 1 2019.
7. Ali, M., Khan, S. U., & Vasilakos, A.V (2015). Security in Cloud computing: Opportunities and challenges. Information Sciences, 305, 357-383.
8. Yara Alghofaili, Albatul Albattah, Noura Alrajeh, Murad A.Rassam, Bander Ali Saleh Al-rimy, Secure Cloud Infrastructure: A Survey on Issues, Current Solutions, and Open Challenges 2021.
9. Naseer Amara, Huang Zhiqui, Awais Ali, Cloud Computing Security Threats and Attacks with their Mitigation Techniques, International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2017.
10. R. Z. W. X. W. Q. A. Z. Minqi Zhou, "Security and Privacy in Cloud Computing: A Survey," in Semantics Knowledge and Grid (SKG), 2010.
11. Moshin, K. Sadaf, H., & Malik, I (2013). Performance Evaluation of Symmetric Crytography Algorithms: A survey. International Journal of Information Technology and Electrical Engineering, 2(2).
12. Chandra Sekhara Reddy T., Prasad D. and Venkateswara Reddy B. IJCTA journal.
13. Dheyab Salman Ibrahim, Enhancing Cloud Computing Security using Cryptography & Steganography, Iraqi Journal of Information Technology, V.9 N.3. 2019.

14. Vipula Madhukar Wajgade, Dr. Suresh Kumar, Enhancing Data Security Using Video Steganography, International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 4, April 2013.

15. R SHANTHAKUMARI and S MALIGA, Dual-layer security of image Steganography based on IDEA and LSBG algorithm in the cloud environment, Indian Academy of Sciences, published in 2019.

16. Santosh Kumar Singh, Dr. P.K.Manjhi , Dr. R.K.Tiwari, " Cloud Computing Security Using Steganography" ,JETIR1907G28 Journal of Emerging Technologies and Innovative Research (JETIR), JETIR June 2019, Volume 6, Issue 6 www.jetir.org (ISSN-2349-5162).

17. J. Geelan, "Twenty-one experts define cloud computing," Cloud computing J., vol 2016, pp. 1-5, 2016.

18. P. Mell and T. Grance, "The NIST definition of cloud computing recommendations national inst. Of standards and technology," NIST Special Publication,vol. 145 pp.7 2019.

19. M. Armbrust, et al., "A view of cloud computing," Common of the ACM, vol. 53, pp.: 50-58, April 2010.

20. L. M. Vaquero, L. Rodero-Merino, J.Caceres, M. Linder, "A break in the clouds: towards a cloud definition," ACM Computer Commun. Review, vol.39, pp.:50-55, Jan 2009.

21. R. Buyya, et al., "Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility," Future Generation Comput, vol 25, pp.:599-616, Jun. 2009.

22. D. S. Linthicum, Cloud Computing and SOA Convergence in Your Enterprises: A Step-by-Step Guide, Boston MA:Addison-Wesley Professional, 2009.

23. M. A. Vouk, "Cloud computing – issues, research and implementations," J. of Computing and Inform. Technology, vol.4, pp.:235-246, 2008.

24. Christopher Olive, White Paper: Cloud Computing Characteristics Are Key, GP Strategies Corporation 6095 Marshalee Drive, Suite 300 Elkridge, MD 21075 USA, 2012.

25. Dr. Chinthagunta Mukundha & K.Vidyamadhuri, "Cloud Computing Models: A Survey", Advances in Computational Sciences and Technology, ISSN 0973-6107 Volume 10, Number 5 (2017) pp.747-761.

26. Preeti Barrow, Runni Kumari, Prof Manjula R, "Security in Cloud Computing For Service Delivery Models: Challenges and Solutions", International Journal of Engineering Research and Applications, ISSN: 2248-9622, Vol 6, Issue4, (Part - 2) April 2016, pp.77-85.

27. " Cloud computing service and deployment models: layers and management", Choice Reviews Online, vol. 50, no. 07, pp. 50-3896-50-3896, 2013.

28. Deririck Rountree, Ileana Castrillo, in The Basics of Cloud Computing 2014, link to article: https://www.sciencedirect.com/topics/computer-science/cloud-deployment-model.
29. P., Mell, T., Grance ."The NIST definition of cloud computing", [Online], Available: http://csrc.nist.gov/groups/SNS/cloud computing/cloud-def-v15.doc , 2009. [Accessed: 15-July- 2011].
30. L. Savu, "Cloud Computing: Deployment Models, Delivery Models, Risks and Research Challenges," in Computer and Management (CAMAN), 2011 International Conference on, 2018, pp. 1-4.
31. T., Klančnik, "NIL - In the Core of the Cloud." [Online]. Available: http://www.nil.si/ipcorner/CoreCloud/ [Accessed: 15-Jul-2011].
32. P., Metri G., Sarote. "Privacy Issues and Challenges in Cloud Computing". International Journal of Advanced Engineering Sciences and Technologies (IJAEST), vol. 5, pp.1-6, 2011.
33. "HPC in the Cloud: Frost & Sullivan: Australia Leads Asia Pacific Adoption of Cloud Computing." [Online]. Available: http://www.hpcinthecloud.com/hpccloud/ 2011-05 30/frost_sullivan_australia_leads_asia_pacific_adoption_of_cloud_computing.html [Accessed: 08-Jul-2011].
34. Mervat Adib Bamiah and Sarfraz Nawaz Brohi, "Expolring the Cloud Deployment and Service Delivery Models", International Journal of Research and Reviews in Information Sciences (IJRRIS), Vol 1, No.3, September 2011, ISSN: 2046-6439.
35. CSA, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1" Cloud Security Alliance, 2009 [Online]. Available: http://www.cloudsecurityalliance.org/guidance/csaguide.v1.0.pdf [Accessed: 08-July-2011].
36. Dave Thomas, "Cloud Computing – Benefits and Challenges!", in Journal of Object Technology, vol. 8 no. 3, May - June 2009, pp. 37 – 41 http://www.jot.fm/issues/issue_2009_03/column4/
37. Sandra Durcevic in Business Intelligence, Jan 10th 2019 https://www.datapine.com/blog/cloud-computing-risks-and-challenges/
38. Ramakrishnan Krishnan, "Security and Privacy in Cloud Computing", Master's thesis Western Michigan University 2017.
39. NIST Special Publication 500-292, NIST Cloud Computing Reference Architecture, September 2011
40. Michael Novinson, " 12 Biggest Cloud Threats and Vulnerabilities in 2020", https://www.crn.com/slide-shows/security/12-biggest-cloud-threats-and-vulnerabilities-in-2020/13. June 08, 2020, 11:47 AM EDT.
41. Hayro, "The three goals of Cyber security-CIA Triad Defined", https://www.preferreditgroup.com/2019/08/27/the-three-goals-of-cyber-security-cia-triad-defined/#:~:text=The%20CIA%20Triad%20refers%20to,organizations%20systems%2C%20network%20and%20data.&text=Encryption%20services%20can%20protect%20your,unauthorized%20access%20to%20protected%20data, August, 27, 2019.
42. Karsten Brauer, "Authentication and security Aspects in an international multi-user network", Thesis (UAS), Information Technology, European Computer Science, 2011.

43. Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, Aoying Zhou, "Security and Privacy in Cloud Computing: A Survey", 2010 Sixth International Conference on Semantics, Knowledge and Grids.
44. Malek Najib Omar, Mazleena Salleh, Majid Bakhtiari, "Biometric Encryption to Enhance Confidentiality in Cloud Computing",2014 International Symposium on Biometrics and Security Technologies (ISBAST).
45. Alexandru Butoi, Nicolae Tomai, "Secret sharing scheme for data confidentiality preserving in a public-private hybrid cloud storage approach", 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing.
46. L. Arockiam, S. Monikandan," Efficient Cloud Storage Confidentiality to Ensure Data Security", 2014 International Conference on Computer Communication and Informatics (ICCCI -2014), Jan. 03 – 05, 2014, Coimbatore, INDIA.
47. Munwar Ali Zardari, Low Tang Jung, Nordin Zakaria, "KNN Classifier for Data Confidentiality in Cloud Computing", IEEE,2014
48. http://www.druva.com/documents/Druva-inSync-Security-Q115-R54-10062.pdf (2014).
49. J. B. Bernabe, J. M. Marin Perez, J. M. Alcaraz Calero, F. J. Garcia Clemente and G. M. Perez, "SemanticAware – multitenancy-authorization system for cloud architectures", Future Generation Computer Systems, (2014), vol. 32, pp. 154-167.
50. D. W. Chadwick and K. Fatema, "A privacy preserving authorization system for the Cloud", Journal of Computer and System Sciences, (2012), vol. 78, no. 5, pp. 1359-1373.
51. A. Saldhana, R. Marian, A. Barbir and S. A. Jabbar, OASIS Cloud Authorization (CloudAuthZ) TC [DB/OL] 2018.
52. http://www.wuala.com/en/learn/technology, (2014-01-03).
53. G.Jaspher W. Kathrine, "Cloud Security Mechanisms for Data Protection: A Survey", International Journal of Multimedia and Ubiquitous Engineering, September 2014.
54. Man-in- the cloud (MITC) attacks; risks and solution, https://www.google.com/amp/s/www.cloudmask.com/blog/man-in-the-cloud-mitc-attacks-risk-and-solution%3fhs_amp=true , CloudMask Team, Aug 11, 2015 2:27:00.
55. Y. Desmedt, Man-in-the-middle attack, in: Encyclopedia of cryptography and security, Springer, 2011, pp. 759–759.
56. B. Potter, B. Fleck, 802.11 Security, O'Reilly Series, O'Reilly Media, Incorporated, 2002. URL https://books.google.com.sa/books?id=RVQ4GgKeEtgC
57. Anurag Kahol, CTO, Bitglass, "Beware the man in the cloud: How to protect against a new breed of cyberattack.", https://www.helpnetsecurity.com/2019/01/21/mitc-attack/, January 21, 2019.
58. P. Kumar and V. K. Sharma, "Data security dependent on steganography and cryptography strategies: An audit," International Journal, vol. 4, no. 10, 2014.
59. Cyber Security, "What is data encryption? Which all are the top encryption algorithms?" https://acodez.in/data-encryption-algorithms/ , jan 17, 2020.
60. Shabir A.Parah, ….Javaid A.Sheikh, "Secure and reversible data hiding scheme for healthcare system using magic rectangle and a new interpolation technique", 2019.
61. GADDE SWETHA & K. JANAKI, "A SURVEY: DATA SECURITY IN CLOUD USING CRYPTOGRAPHY AND STEGANOGRAPHY", Journal of Applied Science and Computations, ISSN NO: 1076-5131, Volume VI, Issue VI, JUNE/2019.

62. Harpreet Kaur, and Jyoti Rani, “A Survey on different techniques of steganography”, MATEC Web of Conferences / 57, 02003 (2016), ICAET 2016.
63. R. J. Mstafa and I. Studen, “A High Payload Video Steganography Algorithm in DWT Domain Based on BCH Codes (15, 11),” (2015).
64. Prof Dr. P. R Deshmukh, and Bhagyashri Rahangdale “Data hiding using video steganography”, Vol. 3 Issue 4, April – 2014 International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 International Journal of Engineering Research & Technology (IJERT).
65. https://www.djangoproject.com/, 9/16/2021, 5:58am.
66. https://www.sam-solutions.com/blog/iaas-vs-paas-vs-saas-whats-the-difference/ , 9/16/2021, 6:30pm.
67. Amel Elamin Elsheikh Elamin, Secure Data on HTML Web Page using Steganography with Encryption and Compression Technique, Sudan university of science and technology repository, College of computer science and information technology, 2019.
68. Sneha Ghoradkar, Aparna Shinde Review on Image Encryption and Decryption using AES Algorithm, National Conference on Emerging Trends in Advanced Communication Technologies (NCETACT-2015).
69. Gaj, K., & Chodowiec, P. (2001, April). Fast implementation and fair comparison of the final candidates for Advanced Encryption Standard using Field Programmable Gate Arrays. In Cryptographers’ Track at the RSA Conference (pp. 84-99). Springer Berlin Heidelberg.
70. Stallings, W. (2006). Cryptography and network security: principles and practices. Pearson Education India.
71. Yenuguvanilanka, J., & Elkeelany, O. (2008, April). Performance evaluation of hardware models of Advanced Encryption Standard (AES) algorithm. In Southeastcon, 2008. IEEE (pp. 222-225).
72. Mohamed, A. A., & Madian, A. H. (2010, December). A Modified Rijndael Algorithm and it's Implementation using FPGA. In Electronics, Circuits, and Systems (ICECS), 2010 17th IEEE International Conference on (pp. 335-338).
73. Pramstaller, N., Gurkaynak, F. K., Haene, S., Kaeslin, H., Felber, N., & Fichtner, W. (2004, September). Towards an AES crypto-chip resistant to differential power analysis. In Solid-State Circuits Conference, 2004. ESSCIRC 2004.
74. F.Collin,\Encryptpic," http://www.winsite.com/bin/Info?500000033023, 2019..
75. G. Pulcini, \Stegotif," http://www.geocities.com/SiliconValley/9210/gfree.html, 3:11pm, 2017.
76. T. Sharp, \Hide 2.1, "www.sharpthoughts.org, 12;00am,2019